



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 #21-1

February 10, 2021 12:00 p.m. – 4:00 p.m. EDT **WebEx Meeting**
DER Forum February 11, 2021 8:00 a.m. – 2:00 p.m. EDT **WebEx Meeting**

Dial-In: 415-655-0003 (USA) / 416-915-6530 (Canada)

Day 1 - RSC Business:

Guest Code: 1783851368

Password: 3iSSaFjc@67 (34772352 from phones)

[WebEx Link](#)

Day 2 - DER Forum:

Guest Code: 1787258377

Password: E8Dn4xfnX@3 (38364936 from phones)

[WebEx Link](#)

For Reference:

[Glossary of Terms Used in NERC Reliability Standards](#), dated January 4, 2021

[NPCC Glossary of Terms](#), dated October 2, 2019

Introductions and Chair's Remarks- COVID-19, NERC and FERC

NPCC Antitrust Compliance Guidelines

Agenda Items:

1.0 Review of Agenda

2.0 RSC Meeting Minutes (Approval Item)

3.0 Items Requiring RSC Discussion

3.1 [NPCC DER Guidance Revision](#)

3.2 [FERC Activities](#)

3.3 [NPCC 2021 Corporate Reliability Goals](#)

4.0 NERC Reliability Standards

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

4.1 Currently Posted Projects

Project	Comment Period End Date	Ballot Period End Date
<u>Project 2015-09 Establish and Communicate System Operating Limits</u> Dean Laforest from ISO-NE @ 12:15 PM	12/7/20 (F)	12/7/20 (A)
<u>Project 2016-02 Modifications to CIP Standards</u> Norm Dang from IESO @ 12:30 PM	12/16/19 (F)	4/6/20 (F)
<u>Project 2017-01 Modifications to BAL-003-1.1</u> David Lemmons from Cooper Compliance @ 12:45 PM	4/17/19 (I)	10/24/19 (F)

<u>Project 2019-02 BES Cyber System Information Access Management</u> William Vesely from Con Edison @ 1:00 PM	9/21/20 (F)	9/21/20 (A)
<u>Project 2019-04 Modifications to PRC-005-6</u> Giannuzzi Giuseppe from HQ @ 1:15 PM	2/26/21 (F)	
<u>Project 2019-06 Cold Weather</u> Matthew Harward @ 1:30 PM	3/12/21 (F)	3/12/21 (I)
<u>Technical Rationale for Reliability Standards</u> Project is on hold	4/20/20 (I)	4/20/20 (I)
<u>Project 2020-02 Transmission-connected Dynamic Reactive Resources</u> Latrice Harkness @ 1:45 PM	5/13/20 (I)	
<u>Project 2020-03 Supply Chain Low Impact Revisions SAR</u>	6/3/20 (I)	
<u>Project 2020-04 Modifications to CIP-012</u>	6/11/20 (I)	
<u>Project 2020-05 Modifications to FAC-001-3 and FAC-002-2 SAR</u>	12/11/20 (I)	
<u>Project 2020-06 Verifications of Models and Data for Generators SAR</u>	1/14/21 (I)	
Comments: (I) – Informal; (F) – Formal; (N) – Nomination Period Ballots: (I) – Initial; (A) – Additional; (F) – Final		

- 4.2 Ballot History (Since last RSC Meeting)
- 4.3 Comment Form History (Since last RSC Meeting)

5.0 **NPCC Non-Standards**

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

- 5.1 Items for Discussion
 - 5.1.1 Directory#7 Approved.
 - 5.1.2 Directory#1 Design and Operation of the BPS --- Review
 - 5.1.3 Directory#12 UFLS --- Retirement
 - 5.1.4 Executive Tracking Summary

6.0 **RSC Member Items of Interest**

- 6.1 RSC Roster

7.0 **Standards Activity Post NERC BOT Approval**

(Since last RSC Meeting)

- 7.1 NERC Filings to FERC
<http://www.nerc.com/FilingsOrders/Pages/default.aspx>
- 7.2 FERC Orders / Rules
<http://www.nerc.com/FilingsOrders/Pages/default.aspx>
- 7.3 Federal Register
<https://www.federalregister.gov/>
- 7.4 [FERC Sunshine Act Meeting Notice](#)
- 7.5 [FERC Open Meeting Summaries](#)

8.0 **NERC Meetings**

8.1 Standards Committee (SC)

<http://www.nerc.com/comm/SC/Pages/default.aspx>

January 20 th – Call	February 17 th – Call	March 17 th – Call
April 21 st – Call	May 19 th – Call	June 16 th – Denver, CO (Xcel Energy)
July 21 st – Call	August 18 th – Call	September 23 rd – Salt Lake City, UT (WECC)
October 20 th – Call	November 17 th – Call	December 15 th – Atlanta, GA (NERC)

8.2 Board of Trustees (BOT) Meeting

<http://www.nerc.com/gov/bot/Pages/Agenda-Highlights-and-Minutes-.aspx>

February 5-6 - Meeting	May 13-14 - Meeting	August 19-20 – Conference Call
November 4-5 – Conference Call		

9.0 **NERC Items of Interest** (Since last RSC Meeting)

9.1 Lessons Learned

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

9.1.1 There has been no new Lesson Learned issued since the last RSC meeting.

9.2 Alerts

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

There has been one new NERC Alerts released since the last RSC meeting.

9.3 NERC Reliability and Security Guidelines

<https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx>

9.4 NERC Rules of Procedure

<https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx>

10.0 **Other Items of Interest**

10.1 NPCC Board of Directors Meeting (BOD) 2021

January 27 th – SGR Law Offices, Jacksonville, FL	March 17 th - Call	May 5 th – NPCC Office
June 2 nd – Call	June 23 rd – NPCC Office	August 4 th – Call
September 1 st and 2 nd – Pierce Atwood	October 27 th – Call	December 1 st – Halifax, NS

10.2 [NPCC 2021 Business Plan and Budget Schedule](#)

10.3 [Idaho National Labs – Communications – Brad Nelson](#)

11.0 Future RSC Meetings and Conference Calls

11.1 RSC 2021 Meeting Dates

February 10 th -11 th , NYC or WebEx
May 12 th -13 th , Saratoga Springs NY or WebEx
August 11 th -12 th Toronto/Montreal or WebEx
October 13 th -14 th Toronto/Montreal or WebEx
December 9 th General Meeting or WebEx

Day Two DER Forum:

February 11, 2021 8:00 a.m. – 2:00 p.m. EDT

12.0 Distributed Energy Resources (DER) Forum Topics

- 12.1 Chair Opening Remarks, Antitrust Guidelines, Meeting Protocols - Guy V. Zito, NPCC Chair of the RSC and DER Forum (8:00 am – 8:10 am)
- 12.2 Offshore Wind Protection System Philosophy presentation by Marie Faber Frølich/ Behzad Sedaghat from Orsted, Denmark (8:10 am - 9:00 am)
- 12.3 TFSP System Protection presentation by Anthony Napikoski from UI/NPCC TFSP Chair (9:00 am - 9:30 am)
- 12.4 Advanced Inverter Functions - IEEE 1547-2018 and the testing standard 1547-2020 presentation by Andy Hoke from NREL (9:30 am - 10:15 am)
- 12.5 PRECISE – a distribution optimizing tool for DER to determine settings for inverters - Adarsh Nagarajan from NREL (10:15 am - 11:00 am)

Break for 15 minutes

- 12.6 Blackstart using inverter - based resources presentation by Himanshu Jain from NREL (11:15 am - 12:00 pm)
- 12.7 Harmonics and power quality presentation by David R. Mueller from EnerNex (12:00 pm - 12:45 pm)
- 12.8 NERC SPIDERWG Updates and NERC IRPWG Battery Energy Storage System and Hybrid Plant Guideline presentation by Ryan Quint (12:45 pm – 1:30 pm)
- 12.9 NPCC DER Guidance Document and Chair Closing Remarks – Guy V Zito, NPCC Chair of the RSC and DER Forum (1:30 pm – 2:00 pm)

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 Assistant Secretary, Ruta Skučas, Esq. at 1-202-530-6428.

Public Announcement

RSC and DER Forum Meetings, WebEx, and Conference calls:

Participants are reminded that this meeting, WebEx, and conference call are public. The access number was posted on the NPCC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.



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 #20-5

December 3, 2020 12:00 p.m. – 4:00 p.m. EDT **WebEx Meeting**

Dial-In: 415-655-0003 (USA) / 416-915-6530 (Canada)

Guest Code: 1785761597

Password: qsGrM9pT\$88 (77476978 from phones)

[WebEx Link](#)

For Reference:

[Glossary of Terms Used in NERC Reliability Standards](#), dated October 8, 2020

[NPCC Glossary of Terms](#), dated October 2, 2019

	Name	Organization	Sector(s)	Day(s)
1.	Guy Zito	Northeast Power Coordinating Council		1
2.	Gerry Dunbar	Northeast Power Coordinating Council		1
3.	Ruida Shu	Northeast Power Coordinating Council		1
4.	Kal Ayoub	FERC	Guest	1
5.	Allen Schriver	Proxy for NextEra Energy		
6.	Avani Pandya	Consolidated Edison Co. of New York, Inc.	4	1
7.	Ben Wu	Orange and Rockland	3	1
8.	Brian Robinson	Utility Services, Inc.	5	1
9.	Chantal Mazza	Hydro Quebec	2	1
10.	Constantin Chitescu	Ontario Power Generation	4	1
11.	Chris Moir	Ontario Power Generation	Guest	1
12.	Cristhian Godoy	Consolidated Edison Co. of New York, Inc.	5	1
12.	Dave Kwan	Ontario Power Generation	4	1
13.	David Burke	Orange and Rockland	3	1
14.	David Kiguel	Independent	7	1
13.	Donald Nelson	Mass DPU	Guest	1
14.	Glen Smith	Entergy Services	4	1
15.	Herb Schrayshuen	Power Advisors, LLC	Guest	1
16.	Jim Grant	NYISO	2	1
17.	Joel Charlebois	AESI, Inc.	7	1
18.	John Pearson	ISO-NE	2	1

19.	Junji Yamaguchi	Hydro Quebec	2	1
20.	Lodie White	FERC	Guest	1
21.	Mike Jones	National Grid	3	1
22.	Mike Ridolfino	Central Hudson Gas and Electric	1	1
23.	Michele Tondalo	The United Illuminating Company	1	1
24.	Nick Parrotta	PLM	Guest	1
25.	Payam Farahbakhsh	Hydro One Networks	1	1
26.	Quintin Lee	Eversource	1	1
27.	Rob Vance	New Brunswick Power	1	1
28.	Salvatore Spagnolo	NYPA	4	1
29.	Sean Bodkin	Dominion	4	1
30.	Sean Lagan	IESO	2	1
31.	Timothy Kucey	PSEG	4	1
32.	Vijay Puran	New York State Department of Public Service	6	1
33.	Norm Dang	IESO	Guest	1
34.	Bill Shultz	Southern Company	Guest	1
35.	Giannuzzi Giuseppe	Hydro Quebec	Guest	1
36.	William Vesely	Consolidated Edison Co. of New York, Inc.	Guest	1

Introductions and Chair's Remarks- COVID-19, NERC and FERC

NPCC Antitrust Compliance Guidelines

The NPCC Antitrust Compliance Guidelines were read by Ruida Shu.

Agenda Items:

1.0 Review of Agenda

Guy Zito provided an update on the COVID-19 situation and update the group regarding the DER forum for next year.

Guy Zito added section 3.4, 3.5, and 3.6 to the meeting agenda.

Mike Jones also added section 3.7 to the meeting agenda.

2.0 RSC Meeting Minutes (Approval Item)

Approval of Agenda-No revision is necessary to the draft RSC meeting agenda.

Brian Robinson made the motion for approval.

Ben Wu seconded the motion.

The meeting minutes were approved as read.

3.0 Items Requiring RSC Discussion

3.1 NPCC DER Guidance Revision

Mike Jones, Herb Schrayshuen and Quintin Lee volunteered themselves to assist in the ongoing effort of DER guidance revision.

3.2 RSC Scope of Work (For RSC to Approve)

Approval of RSC Scope of Work.

Quintin Lee made the motion for approval.

Jim Grant seconded the motion.

The RSC Scope of Work were approved as read.

3.3 RSC Work Plan (For RSC to Approve)

Approval of RSC Work Plan.

Quintin Lee made the motion for approval.

Jim Grant seconded the motion.

The RSC Work Plan were approved as read.

3.4 NPCC 2021 RSC Goal Discussion

Guy Zito provided an overview of the proposed RSC goals for next year.

3.5 FERC Technical Conference Offshore Wind

Decarbonization goals are very aggressive in some states.

Could potentially result in lawsuits if decarbonization goals are not met.

3.6 NOPR on Facility Ratings

A staggered approach is suggested to implement the appropriate equipment for facility line ratings.

Managing transmission line ratings could be an order down the road.

<https://www.ferc.gov/media/rm20-16-000>

Docket No: RM20-16-000

3.7 Non-endorsed Implementation Guidance

FYI, form NERC's filing to FERC. NERC is collaborating with the Regional Entities in developing the CMEP Practice Guide and plans on issuing the Virtualization CMEP Practice Guide by February 2021.

4.0 NERC Reliability Standards

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

4.1 Currently Posted Projects

Project	Comment Period End Date	Ballot Period End Date
Project 2015-09 Establish and Communicate System Operating Limits Dean Laforest from ISO-NE @ 1:00 PM	12/7/20 (F)	12/7/20 (A)
Project 2016-02 Modifications to CIP Standards Norm Dang from IESO 1:15 PM	12/16/19 (F)	4/6/20 (F)
Project 2017-01 Modifications to BAL-003-1.1 Bill Shultz from Southern Company @ 1:30 PM	4/17/19 (I)	10/24/19 (F)
Project 2019-02 BES Cyber System Information Access Management	9/21/20 (F)	9/21/20 (A)

William Vesely from Con Edison 1:45 PM		
Project 2019-04 Modifications to PRC-005-6 Giannuzzi Giuseppe from HQ @ 2:00 PM	7/8/20 (F)	
Project 2019-05 Modifications to PER-003-2 Project is currently on hold pending action from PCGC	8/30/19 (I)	
Project 2019-06 Cold Weather Matthew Harward @ 2:15 PM	5/21/20 (F)	
Technical Rationale for Reliability Standards Project is on hold	4/20/20 (I)	4/20/20 (I)
Project 2020-01 Modifications to MOD-032-1 SAR	4/24/20 (I)	
Project 2020-02 Transmission-connected Dynamic Reactive Resources SAR	5/13/20 (I)	
Project 2020-03 Supply Chain Low Impact Revisions SAR	6/3/20 (I)	
Project 2020-04 Modifications to CIP-012 SAR	6/11/20 (I)	
Project 2020-05 Modifications to FAC-001-3 and FAC-002-2	12/11/20 (I)	
Comments: (I) – Informal; (F) – Formal; (N) – Nomination Period		
Ballots: (I) – Initial; (A) – Additional; (F) – Final		

Project 2015-09 Establish and Communicate System Operating Limits:

Ruida Shu provided a brief update on the project status.

The standard drafting team plans to have a meeting on December 14, 2020 to review the comment questions.

They also plan to have a standard drafting team meeting in early January 2021 to work on FAC-014.

The goal is to post the documents during the first two weeks of February 2021.

Project 2016-02 Modifications to CIP Standards:

Norm Dang called in at 1:15 PM and presented on Project 2016-02.

Project 2016-02 SDT will continue to interface with the Project 2019-02 SDT (BCSI in Cloud) that is revising CIP-004-7 and CIP-011-3.

Based on positive feedback from September 30, 2020, Technical Seminar on the proposed changes to CIP-005, CIP-007, and CIP-010, the SDT will proceed to propose the needed conforming changes to CIP-002 through CIP-013.

First formal posting of the proposed changes scheduled for late January to early February 2021.

The first posting will consist of the complete set of proposed virtualization changes for CIP-002 to CIP-013.

Three formal postings scheduled for 2021.

The SDT hopes to complete by the end of December 2021.

The SDT is looking at the wording for a phase implementation plan where entities that want to proceed with the early virtualization may do.

CIP-002 R1 and CIP-006 R1 conforming changes are more involved.

Project 2017-01 Modifications to BAL-003-1.1

Bill Shultz from Southern company called in at 1:30 PM and provided a presentation to the group.

Phase 1 complete, BAL-003-2 became effective December 1, 2020, and Phase 2 is in process. The standard drafting team looking for industry input on possible modifications to the standard. Relevant discussion topics are: Multiple BA Interconnections, Measurement Accuracy, Resource Variability, Fast Frequency Response, New Generation Resources, Load response reaction to frequency, FERC Order 842, Generator Governor Surveys, BAL-001-TRE solution, Market Based Solutions, and Adequacy of Current Frequency Response – Trends in PFR. New BA requirement – requires an Operational Planning process to address Frequency Responsive Reserve. New BA requirement – specify minimum governor settings or request governor settings from the GO. If the BA specifies a governor requirement, then an additional requirement for a process to allow for exceptions would also be recommended by the SDT. New GO requirement – governor settings specification - meet the BA specification set above New GO requirement – communicate governor settings – as requested New GO requirement – performance requirement - Response to frequency event based on operational status. New BA Requirement - BA calculates the GO performance if the GO performance requirement is added. New GOP requirement – Ensure the unit is operating with the governor responsive or the BA has been notified that it is not responsive (like VAR-002) Date of White Paper, the posting is being determined: Middle of this month or after the holidays

Project 2019-02 BES Cyber System Information Access Management:
William Vesely called in at 1:45 PM and provided an update on the project.
Project 2019 is waiting for Project 2016-02 to move forward to continue with this project.
The SDT wants to keep the standard on the “firm” level.

Project 2019-04 Modifications to PRC-005-6:
Giannuzzi Giuseppe called in at 1:50 PM and provided an update on Project 2019-04.
The standard drafting team held one meeting since the last RSC meeting.
The standard drafting team reviewed the SAR.
Next Thursday, December 10, 2020, at 11 AM eastern time, the standard drafting team will have the next drafting team meeting to discuss the comments from IEEE.
The issue is in table 1.4 and the drafting team is looking for a way to put it into technical guidance instead of having it in the standard.
There is also a concern regarding the battery.

Project 2019-06 Cold Weather
Ruida Shu provided a brief update on the status of Project 2019-06.
The drafting team proposed the following new language for EOP-011-1 section 1.2: The Generator Owner shall keep the most recent cold weather preparedness plan(s); that shall include a revision history specifying changes and dates of review; and most recent data and evidence in support of all Part of Requirement R7
1.3: Provisions for notification of BES generating unit-specific minimum design temperature or minimum demonstrated historical performance during cold weather, including but not limited to:
1.3.1. BES generating unit operating limitations during cold weather
1.3.2. Expectation when BES generating unit status or degradation that impacts system reliability may result from local forecasted cold weather.

The requirement is also added to TOP-003-4.

EOP-011-1: Made modifications to R7: Each Generator Owner shall develop, maintain, and implement one or more cold weather preparedness plan(s) for its BES generating unit(s). The cold weather preparedness plan(s) shall include the following, at a minimum: [Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-Time Operations]

7.1 BES generating unit(s) freeze protection measures based on unique factors such as geographical location and configuration.

7.2 Annual maintenance and inspection of Generating unit(s) freeze protection measures.

7.3 Generating unit(s) weather data

The project is under quality review for early January 2021 posting.

4.2 Ballot History (Since last RSC Meeting)

Ruida Shu reviewed the Ballot History document in the meeting.

4.3 Comment Form History (Since last RSC Meeting)

Ruida Shu reviewed the Comment Form History document in the meeting.

5.0 NPCC Non-Standards

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

5.1 Items for Discussion

5.1.1 Directory#7 Status of Task Force Review

The RCC approved the revised version of Directory#7 at its meeting on December 1, 2020. Task Force revisions include:

- Renamed the document title to ‘Remedial Action Schemes’.
- Aligned the existing regional review process to facilitate compliance with PRC-012-2.
- Revisions to the RAS approval process within NPCC for a Type I and Type II RAS.
- Clarified the language surrounding exceptions to the NPCC more stringent criteria.
- Alignment of the definition for a Limited Impact RAS (Type III) with the NERC footnote in PRC-012-2 to highlight containment within the local area.
- Added security criteria for a Type I RAS.
- The definition of the existing NPCC Glossary term ‘Special Protection Systems’ will be replaced by ‘See NERC RAS’ to reflect the adoption of the NERC Glossary term for Remedial Action Scheme (RAS).
- The Task Forces considered the incremental reliability benefit and cost effectiveness of the reliability criteria contained in Directory #7.

5.1.2 Executive Tracking Summary

5.2 Items for Approval

6.0 RSC Member Items of Interest

6.1 RSC Roster

7.0 **Standards Activity Post NERC BOT Approval**

(Since last RSC Meeting)

- 7.1 NERC Filings to FERC
<http://www.nerc.com/FilingsOrders/Pages/default.aspx>
- 7.2 FERC Orders / Rules
<http://www.nerc.com/FilingsOrders/Pages/default.aspx>
- 7.3 Federal Register
<https://www.federalregister.gov/>
- 7.4 [FERC Sunshine Act Meeting Notice](#)
- 7.5 [FERC Open Meeting Summaries](#)

8.0 **NERC Meetings**

- 8.1 Standards Committee (SC)
<http://www.nerc.com/comm/SC/Pages/default.aspx>

January 22 nd – Call	February 19 th – Call	March 19 th – Atlanta GA (NERC)
April 22 nd – Call	May 20 th – Call	June 17 th – Denver, CO (Xcel Energy)
July 22 nd – Call	August 19 th – Call	September 24 th – Conference Call
October 21 st – Call	November 19 th – Call	December 9 th – Conference Call

- 8.2 Standards Committee (SC) 2021

January 20 th – Call	February 17 th – Call	March 17 th – Call
April 21 st – Call	May 19 th – Call	June 16 th – Denver, CO (Xcel Energy)
July 21 st – Call	August 18 th – Call	September 23 rd – Joint meeting with CCC, Salt Lake City, UT
October 20 th – Call	November 17 th – Call	December 15 th – Atlanta, GA

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

February 5-6 - Meeting	May 13-14 - Meeting	August 19-20 – Conference Call
November 4-5 – Conference Call		

9.0 **NERC Items of Interest** (Since last RSC Meeting)

- 9.1 Lessons Learned
<http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx>
 - 9.1.1 There have been two new Lesson Learned issued since the last RSC meeting.
- 9.2 Alerts
<http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx>

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

9.3 NERC Reliability and Security Guidelines

<https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx>

9.4 NERC Rules of Procedure

<https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx>

10.0 **Other Items of Interest**

10.1 NPCC Board of Directors Meeting (BOD) 2020

January 29 th – SGR Law Offices, Jacksonville, FL	March 18 th - Call	May 6 th – NPCC Office
June 3 rd – Call	June 24 th – Conference Call	August 12 th – Call
September 2 nd and 3 rd – Conference Call	October 28 th – Call	December 2 nd – Conference Call

10.2 NPCC Board of Directors Meeting (BOD) 2021

January 27 th – SGR Law Offices, Jacksonville, FL	March 17 th - Call	May 5 th – NPCC Office
June 2 nd – Call	June 23 rd – NPCC Office	August 4 th – Call
September 1 st and 2 nd – Pierce Atwood	October 27 th – Call	December 1 st – Halifax, NS

10.3 [NPCC 2021 Business Plan and Budget Schedule](#)

11.0 **Future RSC Meetings and Conference Calls**

11.1 RSC 2020 Meeting Dates

February 12 th -13 th , NPCC Office at New York NY
May 13 th -14 th , WebEx
August 17 th WebEx
October 14 th -15 th , WebEx
December 3 rd WebEx

11.2 RSC 2021 Meeting Dates

February 10 th -11 th , NYC or WebEx
May 12 th -13 th , Saratoga Springs NY or WebEx
August 11 th -12 th Toronto/Montreal or WebEx
October 13 th -14 th Toronto/Montreal or WebEx
December 9 th General Meeting or WebEx

The Meeting is adjourned at 3:15 PM on December 3, 2020.

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 Assistant Secretary, Ruta Skučas, Esq. at 1-202-530-6428.

Public Announcement

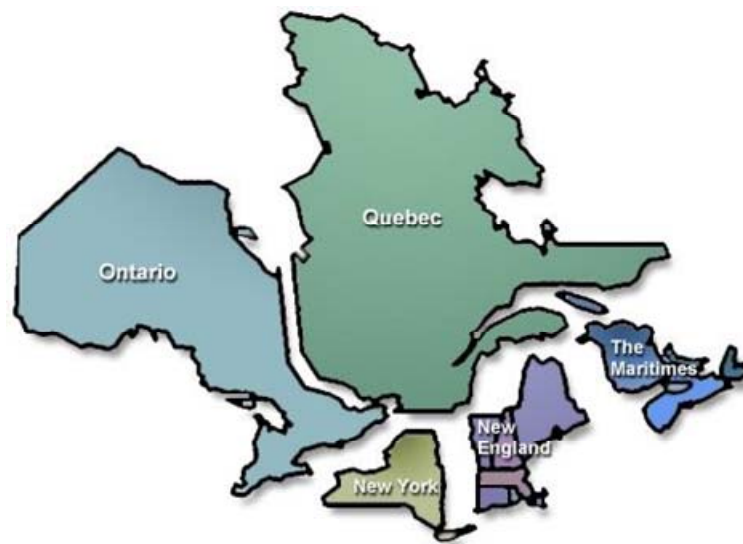
RSC and DER Forum Meetings, WebEx, and Conference calls:

Participants are reminded that this meeting, WebEx, and conference call are public. The access number was posted on the NPCC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.



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

NPCC DER Guidance Document, Distributed Energy Resources (DER) Considerations to Optimize and Enhance System Resilience and Reliability



NPCC Regional Standards Committee (RSC)
Version 2 Approved 11/20/2020

Note: Content of this document may not reflect the most current information¹. Periodic reviews for potential revisions of the document will be done biannually or more frequently if needed. Please send corrections or revision requests to npccstandard@npcc.org.

Contributors:

Jens Boemer	Electric Power Research Institute (EPRI)
David Conroy	Joint Utilities of New York-CMP
David Forrest	EPRI Consultant
James Grant	NYISO
Michael Jones	National Grid (RSC Co-Vice Chair)
Dan Kopin	Utility Services
Benjamin Kroposki	National Renewable Energy Lab (NREL)
Quintin Lee	Eversource (RSC Co-Vice Chair)
Benjamin Loebick	United Illuminating
Brad Marszalkowski	ISO-NE
John Pearson	ISO-NE
Ryan Quint	NERC
Brian Robinson	Utility Services
Herb Schrayshuen	Power Advisors, LLC
Reigh Walling	Walling Energy Systems Consulting, LLC
Guy V. Zito	NPCC (RSC Chair)

NPCC also thanks the Regional Standards Committee (RSC) and the State and Provincial regulatory authorities who provided guidance and information during the development of this document.

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)
1	8/19/19	Effective Date	New
2	X/XX/XX	RSC and Subgroup developed revisions	Revisions, add AGIR, new title, clarifications, and Appendices

¹ The guidance provided in this document is not mandatory, makes no warranty or representations, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in the Material. Additionally, NPCC assumes no liability with respect to the use of, or for damages resulting from, the use of the Material.

Contents

Executive Summary.....	5
Introduction and Objective.....	6
NPCC DER Impact Reporting.....	8
DER BPS Impact Considerations.....	9
NPCC Interconnection Guidance.....	9
Voltage Response.....	12
Frequency Support.....	13
Reconnection to the Utility System	14
Inverters	14
Certification per UL 1741 SA and UL 1741 SB as grid support utility interactive inverters	16
Protective Functions	16
Metering	18
Power Quality.....	19
Power Factor	20
Islanding	20
Automatic Underfrequency Load Shedding (UFLS) Programs	20
Effective Grounding for DER	21
Resource Adequacy.....	22
Energy Storage Systems for DER.....	22
System Control and Data Acquisition (SCADA) and Communications.....	23
DER Recommendations.....	25
Appendix A, NPCC DER Impact Reporting Form and Process	28
Appendix B, NPCC Areas- Comparisons	30
Appendix C – SPIDER Working Group Reliability Guidelines & Activities	31
Appendix D, NPCC Reliability Principles.....	34
Appendix E, State and Provincial AGIR Information	37
New York State.....	37
New England, by State	37
Province of Quebec (some references are only available in French)	40
Province of Ontario	43
Province of New Brunswick	44
Appendix F, ISO New England	45

Appendix G, State Renewable and Green Energy Targets.....	47
Appendix H, Autonomous Energy Grids.....	48

Executive Summary

The Northeast Power Coordinating Council, Inc. (NPCC) is responsible for promoting and enhancing the reliability of the International, interconnected Bulk Power System in Northeastern North America.

Development of this document was initiated by the NPCC Board of Directors to provide regional guidance and information for voluntary use by NPCC Members and stakeholders. The guidance provided herein identifies potential reliability risks² to the Bulk Power Systems (BPS), recommendations to mitigate them, and also identifies opportunities to optimize the operational characteristics of DER to enhance reliability and resilience of the NPCC Bulk Power System (BPS). The document outlines both existing DER deployment practices and strategies as well as how a future with increased penetration of DER and internet controllable devices could be reliably coordinated ([Appendix H](#)). Links to other resources have also been provided throughout the document.

As Distributed Energy Resources (DER) continue to replace traditional industry generation resources the resource fuel mix and operational characteristics of the system will change. DER will necessitate changes to how the system is planned and operated. The North American Electric Reliability Corporation (NERC) Reliability Standards are not applicable to equipment on the distribution systems unless such equipment has a direct impact on the “reliable operation”³ of the BPS, such as Automatic Underfrequency Load Shedding (UFLS). However, as penetration of DER increases, planning and operating assessments used to assure reliable operation of the BPS will need to accurately represent how DER interacts with the BPS.

NPCC recognizes that continent-wide efforts in North America are underway at the NERC level to define DER and address some aspects related to planning and modeling. [Appendix C](#) outlines some specific reliability activities related to DER which have either been developed, or are in the process of being developed, by the NERC System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG), along with links to some of their documents. NPCC and its members have also been engaged in the work efforts at the NERC level and are leading efforts to address outstanding issues within the scope of those groups and provide expertise. With the understanding of all the efforts which are underway, NPCC can coordinate and fill a vital role in identifying additional areas where the Region may provide information and services to promote reliable deployment of DER. An example is coordination with State and Provincial Government Regulatory Authorities, and distribution utilities. Also, opportunities exist in the areas of obtaining data, models, testing and verification, observability, protection systems and other operational characteristics of DER and their effect on the distribution systems.

² An example of a reliability risk not addressed is remote dispatch of DER. A significant challenge that has been found by some NPCC members is that DER Operators can be anywhere in the world and that as a result, communications can be significantly delayed, leading to reliability risks. This includes time zone challenges and language challenges,

³ “reliable operation” is defined in 16 U.S. Code § 824o and 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.”

NPCC has also been conducting DER Forums, the purpose of which is to promulgate DER related information, educate, and inform. NPCC's Regional Standards Committee (RSC) and Reliability Coordinating Committee (RCC) have also developed a joint process and a form to report DER related impacts (i.e. during or following an event both enhancing reliability or causing a reliability risk) and analyze and determine if any further actions are needed. The Form and process may be found in [Appendix A](#) and on the NPCC website.

NPCC is not creating new Criteria or Standards through this guidance document. The intent of this document is informational and as NERC's SPIDERWG, and other groups develop their respective guidance documents it will be revised to achieve continued alignment and avoid duplication.

This guidance document contains [DER Recommendations](#), and information provided by NPCC's Members, NERC, the industry, the US National Renewable Energy Labs, the Electric Power Research Institute (EPRI) and information from NPCC Staff. Also, it is important to note that specific distribution utility requirements within NPCC at the local level will supersede any suggested approaches in this document.

Introduction and Objective

A consistent defined term for what type of generating, demand or storage resources are included in DER is not broadly accepted by industry stakeholders. Also, DER is not currently a term that is defined by NERC.

For the purpose of this NPCC guidance document, DER refers to:

Any non-BPS connected real or reactive power resources (generating units, multiple generating units at a single location, distributed generation installations, battery storage systems, etc.) located within the boundary of any distribution utility's service territory, regardless of capacity, allowing individual DER to be captured if they are not aggregated. Some DER technologies are more intermittent in their production characteristics than resources which operate based on a controllable fuel input.

Initially, in the first version of this guidance document, NPCC specified a threshold for inclusion of DER in any regional guidance that would not include individual rooftop solar or individual wind turbines or other DER net metering installations. However, the aggregate effect of these types of DER can have a significant effect on the power system and if not properly understood can impact the reliable operation of the BPS, as we have seen in California subsequent to their Rule 21⁴. NPCC is now beginning to observe aggregations of DER entering into the capacity wholesale markets within the NPCC Region. This

⁴ <https://www.cpuc.ca.gov/Rule21/> Electric Rule 21 is a tariff that describes the interconnection, operating and metering requirements for generation facilities to be connected to a California utility's distribution system. The tariff provides customers wishing to install generating or storage facilities on their premises with access to the electric grid while protecting the safety and reliability of the distribution and transmission systems at the local and system levels.

document will continue to be modified as emerging issues related to DER's deployment, interconnection, planning and operations are identified and technology improves.

This document identifies opportunities for DER related process improvements and addresses potential reliability risks, promotes good utility interconnection practices necessary for reliability, and promulgates information on how DER can enhance reliable operation at the Transmission Distribution interface by providing essential reliability services. In addition, during the development of this document, a review of existing DER related documents was performed and NPCC is working with the NY Interconnection Technical Working Group (ITWG) as well as the Joint Utilities group of NY to align processes where possible. As other related groups and endeavors are identified within the Region, NPCC will monitor and review their activities going forward and will coordinate with the NPCC Areas and its Members, as necessary.

International standards are established to address DER impact on system reliability. IEEE 1547-2018 as amended by IEEE 1547a-2020 brings significant potential benefits to the BPS by requiring that DER provide essential reliability services to ensure stability, reliability, and security. State and Provincial requirements for DER interconnection should also require compliance with IEEE 1547-2018 through inclusion in their respective jurisdictional interconnection agreements.

As DER continues to proliferate on the electric system at the "grid edge" or distribution system, and replace conventional transmission grid connected resources, there is an increasing reliability related need to understand the effect of DER resources on the BPS. It is important to understand how DER is interconnected, planned, operated and how DER interacts with the transmission system.

Reliably and securely integrating DER into the electric system requires a comprehensive multi-pronged approach utilizing perspectives from different disciplines. DER design, modeling, planning, and relay coordination require consideration of jurisdictional issues. The importance of Members working with their respective national, state, and provincial regulatory authorities to help them understand the consequences of and the development of effective DER interconnection requirements is critical. While there may be some broad universal guidelines, the details of effective DER interconnection requirements should be reconciled with the characteristics of the system where the interconnection is taking place. [Appendix B](#) of this document provides a comparison of NPCC's Area requirements, at the time of the Version 1 writing, to help identify opportunities for guidance.

Many, if not most, of the current DER being deployed is theoretically capable of bringing several enhancements to reliability, provided that there are sufficient design specifications and interconnection requirements to implement the benefits. Inverter based DER may use fast, programmable responses to provide benefits to reliability if properly configured and coordinated with the host utility. Coordination must consider effects both on the distribution system and the BPS. The sections below address DER impact on the BPS including aspects of:

- Interconnection guidance
- Voltage response
- Frequency support

- Reconnecting to the utility following faults
- Underfrequency load shedding

While DER presents opportunities to enhance reliability, they also introduce challenges at the Transmission Distribution interface if not deployed correctly. Interoperability with the transmission system is not solely determined at the point of interconnection. Visibility and a level of controllability of DER is essential for transmission operators to maintain situational awareness for reliable operation of the BPS, and for short-term forecasting. Additionally, characteristics of DER such as capacity, intermittent production, location, protection settings, and other parameters must be known for long-term operational performance forecasting and system planning to ensure BPS reliability is maintained. Additionally, the local distribution utility overseeing the interconnection of DER needs to be able to ensure that the DER doesn't cause safety issues for distribution line workers.

Presently there are limited study tools in general use to perform fully integrated studies of transmission and distribution which would allow both systems to be modeled and studied (in steady-state and dynamically) together, although work is underway in this regard. In the shorter term, visibility of the variability of DER capacity could dramatically affect the quality of state estimator information, and methods of improving data and forecasting need to be explored. The U.S. Department of Energy Argonne National Laboratory has a project underway to develop a tool that would Co-simulate Transmission and Distribution systems. The tool being developed will utilize Siemen's Power System Simulator "PSS®E" transmission system analysis tool with EPRI's open sourced distribution system smart grid tool "OpenDSS"([Smart Grid Simulation Tool](#)) using a Python interface. A detailed presentation on this project may be found in the October 2019 NPCC DER Forum meeting materials on NPCC's website. Additionally, some planners in the NPCC Region are moving to composite load models for their simulations and planning activities.

In recognition of both the benefits and challenges associated with DER, the approach taken with this second version of the NPCC DER Guidance Document is to continue to collect interconnection related information within the NPCC Region as well as in other areas of the NERC Electric Reliability Organization (ERO) Enterprise. There are some specific situations where opportunity exists to ensure better coordination across the NPCC Region. The intent of this document is to identify any emerging reliability issues, provide general guidance and information where possible, and offer support to NERC and others North America wide to promote reliable interconnection and operation practices for DER. It is also recognized that DER may not be located optimally and/or in areas where deliverability to load may not be ideal. In this respect any specific information in this document must be considered in conjunction with the requirements of the interconnecting distribution utility.

NPCC DER Impact Reporting

In order to ensure the reliability and resilience of the interconnected BPS in Northeastern North America as DER, both aggregated and single installations, continue to proliferate throughout the distribution systems within the NPCC Region, it is important to have a regional DER impact reporting mechanism. The NPCC Regional Standard Committee (RSC) created an impact reporting form and process that allows entities to report DER impacts and to seek guidance regarding emerging issues and reliability risks that

affect or could affect the reliable performance of the BPS (see [Appendix A](#)). The Word version of the form also is available on the NPCC website at:

[BES Impact Reporting Form](#)

Impact reporting and its associated process provide an orderly mechanism for NPCC to review reliability impacts submitted. A Report will initiate a collaborative review by the Reliability Coordinating Committee and the Regional Standards Committee.

DER BPS Impact Considerations

NPCC's Regional Standards Committee (RSC) and Task Forces (i.e. Task Force on System Studies) reviews of DER as it pertains to the NPCC Region's BPS performance have identified several areas which, going forward, may warrant further and continual monitoring and analysis. NPCC has identified the following items that should be carefully considered as DER levels (total MWs) increase.

- DER performance with respect to voltage and frequency ride through
- DER ability to provide regulation and reserves
- DER dispatch and controllability
- DER availability, quality of forecasting, and verification
- Observability and situational awareness of DER, and the importance of implementing Advanced Metering Infrastructure (AMI) if telemetry is not deployed
- DER impacts on Underfrequency Load Shed programs
- Impacts of DER on System Restoration and Black Start Plans

Although DER markets, both wholesale and dual participation models, are not the focus of this document, due consideration should be given to their structure. Market rules that allow aggregation also vary across the NPCC Region. Some Areas allow injection of the aggregation across their market area while other Areas require specific aggregations to be injected nearest to a transmission node. DER are capable of providing ancillary services that are necessary to support reliability, if there are appropriate market mechanisms and incentives that allow and encourage them to do so. Wide-area aggregation and injection may create challenges for the system planners and operators as well as raise deliverability and operations concerns.

NPCC Interconnection Guidance

This document and any detailed specifications which follow, are intended to provide examples of general information regarding DER interconnection. The examples do not constitute a Regional Criteria (which can only be implemented through NPCC Directories and approval of NPCC's Full Members). There are numerous efforts underway in many forums and regulatory bodies that are expected to create new, more specific guidance⁵. The level of detail and specificity provided is intended to be used as

⁵ At the time of this guidance document development, these include but are not limited to: NERC (e.g. SPIDER WG, Inverter- Based Resources Task Force (IRPTF), Events Analysis, Modelling and Standards process), IEEE (IEEE Std

information and guidance for any NPCC Member Area which may not have yet seen the need to establish detailed operating parameters. This document shares the practices of some Members of NPCC which have already established detailed DER requirements, even in advance of upcoming applicable industry standards due to the rate of penetration of DER in their Area. NPCC Members considering improving or adding to their respective DER guidance documents are encouraged to reach out directly to other NPCC Members which may have already addressed DER related reliability risk issues.

NERC and NPCC have criteria for resource and transmission planning. For transmission, criteria require transmission planners to simulate different transmission system events and ensure the transmission system remains reliable by meeting performance characteristics for these events. If the transmission system does not remain reliable, the planners are required to identify remediation, including upgrades or expansions of the transmission system. One aspect of the simulation is to account for the loss of generation resources. If a significant amount of DER trips or ceases to inject current for the simulated transmission event, the transmission system could become unreliable for that event and require remediation. This can occur in several scenarios such as a peak load day with maximum output from DER like solar PV or a light load spring day where PV solar and small hydro make up a significant percentage of the generation. IEEE Std. 1547-2018 “Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power System Interfaces” addresses this issue by setting the default DER trip settings for Category II at a level that coordinates with NERC standard PRC-024-2 “Generator Frequency and Voltage Protective Relay Settings.” This is the standard that defines ride-through capability for generators connected to the transmission system. Requiring DER to ride-through disturbances, similarly to large generators, would be a significant step towards achieving a robust level of reliability in a cost-effective manner.

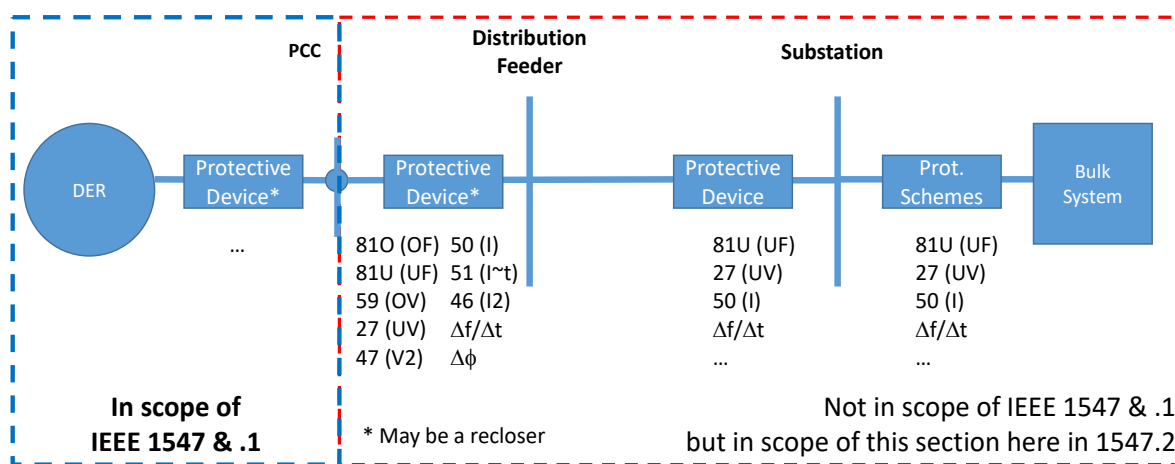


Figure 1: Scope of IEEE 1547 series of standards and guidelines and list of distribution protective functions that may interfere with DER ride-through. Source: Provided courtesy of EPRI⁶

1547.1-2020, P2800), and various state initiatives such as the New York Interconnection Technical Working Group (ITWG), Other regional, Provincial and State initiatives.

⁶ EPRI makes no warranty or representations, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in the Material. Additionally, EPRI assumes no liability with respect to the use of, or for damages resulting from the use of the Material.

IEEE 1547-2018 was unanimously adopted by the National Association of Regulatory Utility Commissioners (NARUC) in 2019. The standard outlines the technical specifications and performance requirements which are universally needed for interconnection and interoperability of DER and should be sufficient for most installations. Implementation guidance for IEEE 1547-2018 may be found here: [Guideline IEEE 1547-2018](#). The applicability of certain specifications and requirements are dependent on specific application considerations. For these, the requirements are provided in terms of a limited number of technology-neutral performance categories, for which it is the responsibility of the authority governing interconnection requirements (AGIR) to consider. Within New England, interconnection requirements vary by state, and further, by Distribution Provider. In New York a common set of DER interconnection requirements exists and there is a Coordinated Electric System Interconnection Request (CESIR) which outlines and initiates the process. Several other State and Provincial AGIR have developed local interconnection requirements which are listed in [Appendix E](#) of this document along with links which will be helpful to access specific interconnection information. These requirements are then supplemented by individual Distribution Provider interconnection agreements, specifications, and requirements.

The DER owner, responsible for its operation, must follow Interconnection Agreements and any AGIR requirements for fault ride-through. Distribution Providers and other AGIR entities should ensure that their requirements describe necessary DER performance with ride-through capabilities for frequency and voltage excursions events. Interconnection Agreements and local requirements generally have provisions to provide documentation upon request.

In addition, NERC developed three NERC Disturbance Reports related to system disturbances in California which resulted in significant inverter-based resource interruptions. The reports may be found on NERC's Major Events Analysis Reports page: <https://www.nerc.com/pa/rrm/ea/Pages/Major-Event-Reports.aspx>. Some of these past events emphasize the importance of fault ride-through.

In terms of generation resource adequacy and resource management there is also the possibility of over generation, as has been demonstrated in the state of California when the system operator runs out of load to absorb the available generation. Operating procedures for selecting which generation to curtail should be in place requiring System Operator visibility of DER either individually or in aggregate. In lieu of operating procedures, some areas of the country are planning to use market mechanisms to address this issue. Interconnection agreements or other state or local requirements may require DER installations to provide communication channels so that generation can be coordinated with a central dispatch authority.

The DER owner's protection and control equipment also should be capable of ceasing to inject current, or automatically disconnecting the generation from the system to which it is directly connected upon detection of frequency or voltage excursion conditions outside of the applicable ride-through requirements. Note that those interconnection agreements, specifications, and requirements should account for both distribution protection and the reliability of the BPS. For three-phase installations, the over and under voltage function should be implemented on each phase and the over and under frequency protection on at least one phase. All phases of a generator or inverter interface should

disconnect or cease to inject current for appropriate voltage or frequency excursion conditions sensed by the protective devices. Voltage protection should be wired as specified by IEEE 1547-2018. Automatic disconnect devices must be sized to meet all applicable local, state, and federal codes.

The specified size of the generation facility or energy storage system should be based on electrical generator or inverter AC nameplate ratings. The specific design of the protection, control, and grounding schemes will depend on the size and characteristics of the DER owner's generation, as well as the DER owner's expected load level. Dynamic protection systems may be needed based on the characteristics of the particular portion of the utility's system where the DER owner is interconnecting.

The settings referenced herein are generally intended for single-phase and three-phase applications using wye grounded- wye grounded service transformers or wye grounded-wye grounded isolation transformers. For applications using other transformer connections, a site-specific review should be performed by the utility and the revised settings identified in the DER Application Process⁷.

The guidance set forth in this document is intended to be consistent with those specifications contained in the most current version of IEEE Std. 1547-2018. It is recommended that the requirements in IEEE 1547-2018 be referenced in the interconnecting utility requirements as well as any further state interconnection requirements as appropriate.

Voltage Response

Within IEEE-1547-2018 and in NY State Public Service Commission Interconnection Requirements, the operating range for the generators is generally intended to be from 0.88 to 1.10 per unit of nominal voltage magnitude. In addition, the generator should not cause the system voltage, at the Point of Common Coupling (PCC), to deviate from a range of 0.95 to 1.05 per unit of the utility system voltage. For excursions outside these limits with a duration longer than the applicable fault ride-through requirements, the protective device generally automatically initiates a disconnect sequence from the utility system as detailed in the most current version of IEEE Std. 1547-2018. Planning Coordinators and Transmission Planners should also be aware that DER installed with older interconnection agreements may reference prior versions of IEEE Std. 1547 and may not meet current ride through requirements. Clearing time is defined as the time the range is initially exceeded until the DER owner's equipment ceases to energize the PCC and includes detection and intentional time delay. Other static or dynamic voltage functions may be permitted or required as agreed upon by the utility and DER owner. The industry is now in the process of promoting ride-through via several different standards initiatives which NPCC is tracking through its DER Forum.

As described above, ensuring that DER can respond appropriately for various voltage conditions is critical for system reliability, as well as avoiding equipment damage and protecting personnel safety. Continuous operation over a wide range of voltage levels will ensure that DER do not prematurely trip or cease to inject current and further deteriorate system conditions. IEEE Std. 1547-2018 includes ranges of

⁷ Currently there has not been an assessment of potential change in sensitivity (increase or decrease) to the effects of Geomagnetic Disturbance (GMD) from the presence of high DER penetration. This is a potential reliability risk to be aware of and evaluated in the future.

trip settings. For inverter-based DER, the “shall trip under” voltage setting should be chosen to meet the requirements of NERC PRC-024-2, as described in Annex B of IEEE Std.1547-2018.

Quebec Interconnection

Ride-through during system disturbances is of primary importance for resources connected to the grid, with the objective of maintaining system reliability⁸. IEEE-1547-2018 addresses the topic, however, for voltage and frequency, what is required in the IEEE standard does not match the requirements in Quebec.

DER should have voltage related operational capability and protection settings set as prescribed by the area Electric Power System (EPS)operator and in accordance with IEEE Std. 1547-2018.

This subject area is a matter of facility installation and personnel policy of the asset owner, balancing both reliability and safety. This information should be communicated to the interconnecting utility for proper protection system coordination.

In the Quebec interconnection voltage ranges and regulation requirements vary from the Eastern Interconnection. The requirements of the AGIR having jurisdiction should be followed (typically the Régie de l'énergie and Hydro-Québec). Details for Quebec’s process may be found in [Appendix E](#).

Frequency Support

Frequency support is provided through the combined interactions of synchronous inertia and frequency response. Working in a coordinated way, these characteristics and services arrest the decline in frequency after a disturbance and eventually return the frequency to the desired level. As increased levels of DER are introduced to the system, synchronous inertia will be displaced, which may have an impact on the frequency response performance of the system. With increased penetration of DER it is becoming desirable for DER to remain connected even outside the prescribed frequency range if there is no risk to the DER equipment. The ride-through curves are “shall not trip within the acceptable range,” not “must trip immediately outside of the acceptable range.”

Interconnection Agreements should require DER to have a frequency and voltage operating range that is equivalent to BPS connected resources consistent with the most limiting of PRC-006-NPCC, PRC-024 and the latest version of IEEE 1547 (IEEE 1547-2018 as amended by IEEE 1547a-2020). The sequence for a protective device to automatically initiate a disconnect sequence from the utility system is also detailed in the IEEE-1547-2018. Clearing time is defined as the time the range is initially exceeded until the DER owner’s equipment ceases to energize the point of common coupling (PCC) and includes detection and intentional time delay. Other static or dynamic frequency functionality may be permitted or required as agreed upon by the utility and DER owner. There should be a mechanism to ensure that the Distribution Provider transmits any necessary information pertaining to capacity, operational characteristics, etc. to system planners and system operators for DER facilities.

Note that in the Quebec Interconnection the frequency operating range is wider than in the Eastern Interconnection. In Quebec, the acceptable steady-state frequency range is from 59.4 Hz to 60.6 Hz, and

⁸ NERC report on Loss of Wind Turbines During System Disturbances : [NERC Report-Loss of Wind Turbines](#)

DER must be capable of riding through frequency as low as 55.5 Hz (for a short time period). Therefore, in Quebec, UFLS systems must operate outside this operating range in accordance with the Quebec variance to the PRC-006-NPCC UFLS-1 regional standard table 4.

Reconnection to the Utility System

If the DER is disconnected as a result of the operation of a protective device, the DER owner's equipment should remain disconnected until the utility's service voltage and frequency have recovered to acceptable voltage and frequency limits for an acceptable amount of time. Interconnection Agreements or local standards should address times for reconnection to the utility system. Per IEEE 1547-2018 Clause 4.10.3, the allowable range of settings is 0-600 seconds with a default setting of 300 seconds. IEEE 1547-2003 in clause 4.2.6 allows an adjustable delay or a fixed delay of 5 minutes. The time specified by the interconnection agreement should be coordinated to support BPS reliability as well as distribution requirements.

DER systems greater than 25 kW that do not utilize inverter-based interface equipment should not have automatic recloser capability unless otherwise approved by the utility. If the interconnecting utility determines that a facility must receive permission to reconnect, then any automatic reclosing functions must be disabled and verified to be disabled during verification testing.

Utilities in other parts of the Eastern Interconnection who have experienced increased levels of DER have determined that during system restoration, DER should not be allowed to return to service until the system has been reestablished and is in a stable operating state. Interconnection Agreements and standards should address necessary communications and SCADA requirements. As traditional resources on the BPS are retired and the grid becomes increasingly reliant on grid edge DER on the Distribution system, Black Start, and System Restoration plans will have to be adjusted accordingly.

Inverters

A power inverter, or inverter, is a power electronic device or circuitry that converts direct current (DC) to alternating current (AC). The inverter itself does not produce power. The power is provided by the DC source. Inverter design and/or configuration should be capable of ride-through for specified utility system events and are grouped into three separate performance Categories.

- Category I is based on minimal BPS reliability needs and is reasonably attainable by all DER technologies that are in common usage today.
- Category II covers minimum BPS reliability needs, and coordinates with NERC Reliability Standard PRC-024-2, which was developed to avoid adverse tripping of BPS generators during system disturbances.
- Category III provides the longest duration and widest range (band) for voltage ride-through capabilities that are attainable by inverter-based systems where very high levels of DER penetration are expected or where momentary cessation requirements are seen as a desirable solution for coordinating with distribution system protection and safety. This category is intended to address DER integration issues like power quality and system overloads caused by DER tripping in the local Area Electric Power System and to provide increased BPS reliability by further reducing the potential loss of DER during bulk system events.

Power Conversion	Prime Mover / Energy Source	Category
Inverter	Solar PV, Battery Energy Storage	Category III ¹ (amended)
	Wind	Category II
	Hydrogen Fuel Cell	Mutual Agreement
Synchronous generator	Bio-/landfill gas, fossil fuel, hydro, combined heat & power	Category I
Induction generator	Hydro	Mutual Agreement
¹ was Category II prior to Amendment		

Figure 2: Example assignment of IEEE 1547 abnormal performance categories to various types of DERs.
Source: Provided courtesy of EPRI⁹

Inverters intended to provide local grid support during system events that result in voltage and/or frequency excursions as described in this document should be provided with the required functionality to allow for the equipment to remain online for the duration of the event.

It is recommended that all applicable inverter-based applications should:

- be certified per the requirements of UL 1741 SA as a grid support utility interactive inverter
- have the voltage and frequency trip settings as specified by the interconnecting utility
- have the abnormal performance capabilities (ride-through)
- provide interactive inverter functions status

In New York State it is recommended that equipment be selected from the Department of Public Service “Certified Interconnection Equipment list” maintained on the NY Public Service Commission’s website. Interconnected DG systems utilizing equipment not found in such list should meet all functional requirements of the current version of IEEE Std. 1547-2018 and be protected by utility grade relays (as defined in these requirements) using settings approved by the utility and verified in the field. The field verification test in New York State must demonstrate that the equipment meets the voltage and frequency requirements detailed in this section. Individual New England State interconnection

⁹ EPRI makes no warranty or representations, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in the Material. Additionally, EPRI assumes no liability with respect to the use of, or for damages resulting from the use of the Material.

standards and agreements also typically refer to IEEE Std. 1547-2018 functional requirements and include protection setting review requirements.

ISO-New England also has developed a technical bulletin, contained in [Appendix F](#), which outlines required settings for inverters in New England.

Certification per UL 1741 SA and UL 1741 SB as grid support utility interactive inverters

Because Inverters currently certified for IEEE 1547-2003 do not currently provide adequate grid support functionality, in the interim period until DER that have been certified as meeting IEEE Std. 1547-2018 in accordance with IEEE Std. 1547.1-2020 (IEEE Standard Conformance Test Procedures for Equipment Interconnecting Distributed Energy Resources with Electric Power Systems and Associated Interfaces) and UL 1741 SB (September, 2020) become available, certification of all inverter-based applications is needed. For example, in one NPCC Area the following approach was taken to assure having inverters installed with a standardized set of grid support functionality to ensure the reliability of the BPS (e.g. maintaining acceptable system frequency and voltage).:

- Should be compliant with only those parts of Clause 6 (Response to Area EPS abnormal conditions) of IEEE Std. 1547.1-2018 (2nd ed.) that can be certified per the type test requirements of UL 1741 SA (September 2016).
- May be sufficiently achieved by certifying inverters as grid support utility interactive inverters per the requirements of UL 1741 SA (September 2016) with either CA Rule 21 or Hawaiian Rule 14H as the Source Requirement Document (SRD). Such inverters are deemed capable of meeting the requirements of this document.
- Applications should have the voltage and frequency trip points and abnormal performance capabilities consistent with IEEE 1547-2018, PRC-024-2 and PRC-006-NPCC “Automatic Underfrequency Load Shedding.”
- For abnormal performance, Category III inverters should be recommended for use. (There may be some circumstances, such as certain types of fuel cells) where the primary energy source may not allow practical implementation of Category III performance. Specification of Category II performance in abnormal conditions may be acceptable in these limited cases.)

UL Standard 1741 Supplement B (UL 1741 SB) implements the test requirements for compliance with IEEE 1547-2018 DER performance requirements in accordance with the test specifications of IEEE 1547.1-2020. With the approval of this UL standard in September 2020, it is anticipated that inverters compliant with IEEE 1547-2018 grid support requirements will be widely available by 2022. Substantial availability of compliant inverters can be anticipated somewhat prior to that date as inverter manufacturers complete their design modifications and move their products through the UL certification process. Once UL 1741 SB inverters become pervasive, the measures in the first and second bullets above are no longer applicable or necessary.

Protective Functions

Protective system requirements for distributed generation facilities result from an assessment of many factors, including but not limited to:

- Type and size of the DER facility
- Voltage level of the interconnection
- Location of the DER facility on the distribution circuit
- Distribution transformer
- Distribution system configuration
- Available fault current
- Load that can remain connected to the DER facility under isolated conditions
- Amount of existing DER on the local distribution system.

Local Interconnection Agreements and standards should require that synchronous, induction and inverter based DER include protection functions for Under/Over Voltage (27/59), Over/Under Frequency (81O/81U), Overcurrent (50P/50G/51P/51G) and Anti-Islanding Protection. Reverse power protection should also be considered as appropriate for BPS support. Interconnection Agreements and standards should require that inverter based DER should be certified according to UL 1741SA as grid supportive. DER protection equipment should utilize a non-volatile memory design such that a loss of internal or external control power, including batteries, will not cause a loss of interconnection protection functions or loss of protection set points. Interconnection Agreements and standards should require that DER protective devices utilize their own current transformers and potential transformers for protection and not share electrical equipment associated with utility revenue metering.

The need for additional protective functions will be determined by the utility on a case- by-case basis. If the utility determines a need for additional functions, it will notify the DER owner of the requirements. The notice should include a description of the specific aspects of the utility system that necessitate the addition, and ideally, explicit justification for the necessity of the enhanced capability. The connecting utility should specify and provide settings for those functions that the utility designates as being required to satisfy their individual protection practices. Any protective equipment or setting specified by the utility is not to be changed or modified at any time by the DER owner without consent from the utility.

The DER owner is responsible for ongoing compliance with all applicable local, state, and federal codes and standardized interconnection requirements as they pertain to the interconnection of DER.

All interface protection and control equipment should operate as specified by state and local interconnection agreements and standards.

In New England, for monitoring and control of new DG projects, [Appendix E](#) lists current interconnection documentation and standards for DER by State. The DER communications hardware, protocols, and data models must comply with these state and local interconnection utility standards.

In New York, for monitoring and control of new DER projects, the most current version of the Monitoring and Control Criteria should be employed by the utilities to evaluate the need for such

equipment in New York. The New York Monitoring and Control Criteria document was developed and agreed to through a collaborative process as part of the Interconnection Technical Working Group (ITWG)¹⁰. The communications hardware, protocols, and data models must comply with local interconnection utility standards.

Also, and fundamentally, existing over-current protections in distribution system are typically designed to clear line and ground faults occurring downstream from their location, as the only source feeding the fault is the transformer station. Connecting a DER provides another source supplying the fault, and the fault contribution from the facility might cause protection to operate non-selectively for reverse faults, out of the protected zone. If the maximum reverse fault current through a non-directional fault-interrupting device exceeds the setting of the device, the fault-interrupting device should be considered with a directional feature to prevent tripping for reverse fault current flow. For instance, phase protection could be replaced with an impedance relay (function 21) if required.

Metering

Advantages and Opportunities of Implementing Advanced Metering Infrastructure (AMI):

IEEE 1547-2018 interoperability requirements specify that the DER have communication capabilities and shall measure specific quantities and have this information available at the communications interface. Most utilities, however, do not have and are not requiring DER owners to provide the communications needed to connect all DER to a grid SCADA system. Such requirements tend to be placed only on large DER. Most utilities do not have the information infrastructure necessary to interoperate with large numbers of small DER; however, implementation of AMI will help in this regard.

Depending on the level of analytics utilized by an Electric Distribution Company (EDC), AMI can provide varying levels of intelligence and operability about the electric distribution system. Even if no analytics are implemented, value can be gained by reviewing and having access to the data provided by AMI. If a full-fledged data analytics package is implemented, then significant benefits can be realized.

Without an analytics package, engineers or analysts can still review basic voltage information provided from AMI. Using SAS, Excel or other simple tools, the voltage data provided, on a daily basis, can be quickly filtered down to exhibit meters that have high or low voltages exceeding the limits set by local Regulatory bodies. With minimal research, it can be determined if high voltage is caused by the presence of DER, either for the meter affected or a nearby neighbor on the same secondary transformer. The transformer can be evaluated by engineering to determine if new, larger equipment is needed.

With reports of abnormal voltage, Distribution Planning can evaluate the data and determine if voltage regulators need to be added towards the end of a circuit, if switching needs to occur to change circuit topology, or if other actions are needed. If the low voltage only occurs at certain times of the day, then perhaps load tap changers at the substation may be used to address the issue.

¹⁰ This document can be found on the Department of Public Service website (www.dps.ny.gov) at the Distributed Generation/Interconnections tab under Interconnection Technical Working Group Information.

If implementing a data analytics package, whether off-the-shelf or home grown, more details on system operating conditions can be found. For instance, by evaluating the sum of meter usage for a specific transformer, secondary transformers can be determined to be over or under loaded. If voltage interval data is available, the GIS model of the system can be evaluated to identify meters that are incorrectly assigned to transformers; the model can be corrected to properly assign meters to transformers.

With data analytics and near real-time data transfer from the head-end system then volt-var optimization can occur. As LTCs, capacitor banks or voltage regulators are adjusted, live feedback from the system can be evaluated to ensure the expected responses are occurring. If something unexpected is happening, then operators receive evidence of this quickly and can take remedial actions.

The specific benefits of AMI are still evolving, and as more analytical tools are made available, and as meters become more advanced, the data will be leveraged to provide more insights into the operation of the distribution network.

Metering requirements for SCADA purposes are usually determined by the local connecting utility and based on the configuration of the DER system prior to energization. Whether SCADA metering can be integrated with revenue metering is a matter for the local connecting utility and connecting DER facility to decide. New metering or modifications to existing metering should be reviewed on a case-by-case basis and be consistent with metering requirements specified by the local connecting utility and any overarching requirements adopted by the local regulatory authority that has jurisdiction (e.g. state commission for example for revenue metering).

IEEE-1547-2018 requires DER to be capable of providing monitoring of connection status, real power output, reactive power output, and voltage either at the point of connection or some agreed upon point if multiple DER facilities are involved. Going forward, member utilities should consider developing IT Infrastructure plans to aggregate and report critical DER Status to BPS Operators, i.e. aggregate DER output within a given area and map those to individual transmission nodes. This information should be available to the system operator as required by the connecting utility. The monitoring equipment should be installed at the time of interconnection and meet the technical requirements of the connecting utility. The DER metering and monitoring communications will allow interoperability and the capability to provide system operators with situational awareness necessary for reliable operation of the interconnecting utility facilities. As more DER is employed and base load generation is replaced with DER resources, it will be important for the Distribution Provider (DP) or interconnecting utility to be able to monitor the availability and production of electricity (power output and energy delivered) from the DER resources.

Power Quality

In practice, DER-related power quality issues are exclusively distribution issues and have little impact or relevance to the bulk power system, or to power quality in other distribution systems. Therefore, this topic is not addressed in this document.

Power Factor

IEEE 1547-2018 requires new DER to have the capability to produce or absorb reactive power from 0.95 pf leading to 0.95 pf lagging¹¹. The standard also specifies that DER have a number of different control functions to regulate this reactive power capability. Legacy DER are typically operated at unity power factor.

Because of the low reactance to resistance (X/R) ratio of distribution systems, the general impact of DER active (kW) power at high penetration is to elevate distribution voltages, potentially to excessive levels. Utilization of DER reactive power capabilities will generally mean that these DER will be absorbing reactive power during high output in order to hold down the distribution voltage to acceptable levels.

Transmission system voltage are generally decoupled from distribution system voltage levels by on-load tap changers in primary distribution substation transformers. The increased reactive power demand that can be brought about by deployment of DER reactive power to mitigate distribution overvoltage issues, however, can directly impact the transmission system unless that additional reactive power demand is compensated by capacitor banks at the distribution substation bus. This can increase total reactive power demands on the transmission system and could potentially have adverse impacts on bulk system voltage stability.

Islanding

Although an entire distribution substation along with some transmission assets could become islanded in a very high DER penetration scenario, islanding is primarily a distribution system concern. IEEE Std 1547.1-2020 tests certified DER for islanding detection with the most insensitive trip settings and with the most aggressive grid support functions. Because DER must pass the islanding detection tests despite these settings and functions, islanding concerns should not be a constraint on implementing trip settings and disturbance ride-through requirements that are necessary for protecting the bulk system security from the impacts of widespread DER resource tripping due to transmission level disturbances.

Some of the anti-islanding algorithms that are implemented in DER intentionally destabilize islanded systems in order to force voltage or frequency tripping. There is some concern that, at high regional DER penetration, these functions may also have adverse impact on the dynamic stability of the bulk system. This potential issue is in need of research to define its extent and severity.

Automatic Underfrequency Load Shedding (UFLS) Programs

UFLS is implemented to restore power system frequency stability if system frequency drops below the UFLS operational set point. Significant deviations in system frequency typically occur during major disturbances such as a loss of generation or events in excess of design contingencies used for planning purposes. UFLS is considered the “safety net” for the BPS and a last resort automatic operation designed to stabilize BPS islands for a generation deficiency. Various fractions of load are shed in multiple stages, up to about 31% of peak net load¹², in order to stabilize frequency. UFLS is primarily installed on distribution feeders, where DER is increasingly being deployed.

¹¹ Certain DER, such as rotating generators, may be allowed to meet slightly less stringent reactive power requirements.

¹² Peak net load shall be calculated as an average of the peak net load from the previous 3 years, excluding the

NERC has a set of requirements in the PRC-006 standard and NPCC has more stringent requirements in NPCC's Regional Standard, PRC-006-NPCC¹³ which outline expected UFLS performance. Approved and effective versions of these standards may both be found on the NERC website.

SS-38 is the NPCC working group responsible for inter-Area dynamic analysis. The SS-38 Working Group regularly studies the UFLS performance within the Region and has recently completed sensitivity analysis showing that a moderate increase of DER penetration anticipated in the short term will not result in any significant degradation in the UFLS program performance based on the conditions and assumptions used in the analysis.

In the future, adopting a more flexible approach to UFLS may be necessary as DER penetrations reach higher levels. There are utilities that are reviewing the feasibility of "Adaptive UFLS" which uses real time monitoring of distribution feeder loads and their DER to determine how much additional load may need to be tripped when DER has increased output. Some utilities, such as Duke Energy avoid choosing those distribution feeders for the UFLS program that have DER interconnected to them.

Effective Grounding for DER

The subject of Effective Grounding may not, in many cases, be impactful to BES reliability it will potentially have an impact on Substation equipment, particularly substation class metal oxide varistor (MOV) arrestors due to overvoltages during faults. With the onset of high penetrations of DER, such as photovoltaic (PV) generation, utilities should consider interconnection of DER similarly to how they would interconnect synchronous generators.

Conventional generators are considered voltage sources as the magnetic flux within the generator tends to provide a constant voltage source during faults. In contrast, inverter-based DER are considered voltage-controlled current sources during faults. Inverter-based facilities generally provide less short-circuit current than similarly sized synchronous units.

Solidly grounding a transformer neutral for a DER plant eliminates a possible phase overvoltage stemming from a single-line-to-ground fault. A potential problem with the solid grounding in the distribution line is that large fault currents can flow through the transformer neutral, which can desensitize the overcurrent protection coordination. In order to mitigate this issue, impedance grounding can limit the fault current and potential equipment damage, while allowing overvoltage to some limited magnitude. Some utilities protect their distribution from overvoltage by using overvoltage protection so Effective Grounding isn't a concern. Further investigation on the how specific installations are grounded is warranted and being pursued by the Interconnection Technical Working Group (ITWG) in New York.

current year. See NPCC's Regional Standard for further details on UFLS requirements, PRC-006-NPCC-2 [Automatic Underfrequency Load Shedding](#)

¹³ Effective Date of the Standard is 4/1/2020 subject to the Implementation Plan and specific area regulatory approvals

Resource Adequacy

Forecasting resource adequacy is an important system reliability planning function¹⁴. The reporting of generation capability and related performance data is integral to this activity. Specific modelling information of intermittent DER resources is critical to planning and understanding system performance. Information related to DER in-service dates, capacity value, availability, emergency assistance, scheduling, and deliverability should be available to the planners. Modeling, data, and other necessary information should be defined and made available to those needing it, such as system planners and system operators. Any requirements associated with this information should be in Interconnection Agreements or Tariffs prior to any commissioning of the DER. Mechanisms for DER entities to provide this information are evolving, depending on locality, and subject to change as DER penetration increases.

Energy Storage Systems for DER

Battery storage technology is undergoing a rapid evolution from Lead Acid to Absorbent Glass Mat to Li-Ion due to the expanding application of batteries to transportation and other sectors. Li-Ion batteries have been and continue to be deployed in a wide range of electric energy-storage applications, ranging from energy-type batteries of a few kilowatt-hours in residential systems with rooftop photovoltaic arrays to multi-megawatt containerized batteries for the provision of grid ancillary services. The Energy Storage Association (ESA) anticipates at least 35 GW of new energy storage will be deployed in the United States by 2025.

NPCC is also observing marked increases in Hybrid Resources which are combinations of multiple technologies that are physically and electronically controlled by the Hybrid Owner/Operator behind the point of interconnection (“POI”) and offered to the grid as a single resource at that POI. This arrangement usually involves energy storage at a photo-voltaic or wind turbine site. It optimizes the use of DER and enables normally clipped energy (energy beyond the rating of an inverter or unneeded by the BPS) to be stored on-site and released in the future. It also allows low outputs of DER which may be outside the operational range of an inverter to be harvested for charging on-site storage allowing better utilization of the total resource. In the figure below the red curve represents the capability of an inverter and the blue is the capability of the DER. Areas between the curves may be used to charge or be “harvested.” This leads to a more efficient utilization of the DER and supports grid reliability and state of charge of the energy storage. As shown in Figure 3 below, the capability of an inverter can be exceeded by the capability of the DER behind it. Figure 3 below also displays a typical daily capability curve associated with a PV inverter with the maximum power capability delivered during mid-day. DER in many instances is designed with due consideration of the degradation of capability, such as a solar panel’s capacity over time.

¹⁴ For background on resource adequacy metrics see: [“Resource Adequacy Metrics and their Applications”](#) prepared by the New York State Reliability Council.

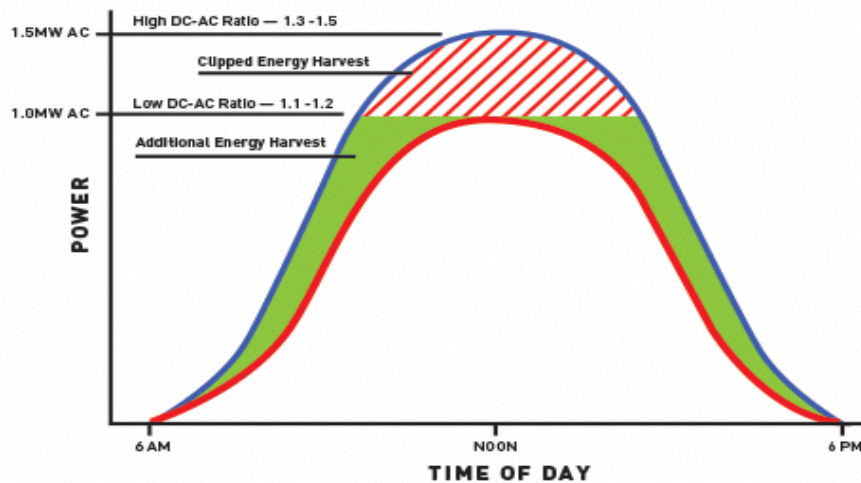


Figure 3- Storage showing Clipped and Unused Energy

The ESA has an online report to manage any risks associated with Energy Storage. Their report may be found here, [Energy Storage, Operational Risk Management](#). Care should be used in placement of batteries and should avoid physical proximity (due to the risk of fire or explosion) and electrical proximity (due to harmonics and other power electronic interaction concerns) to other facilities that may be critical to the reliable operation of the BPS.

System Control and Data Acquisition (SCADA) and Communications

As DER penetration increases all DER above a certain MW level, as determined by the interconnecting utility or System Operators, should be required to provide SCADA telemetry data to a control center to monitor their output. It might be beneficial to have DER data be communicated to a Distribution System Operator, distribution system platform or similar, to provide analysis and aggregation of data for a concise summary to the transmission system operator. IEEE-1547-2018 has a communication port requirement. This ensures that the output remains visible to the system operator. It allows the system operator to observe DER status when working on a feeder in emergency or planned outage situations. Some NPCC Members have encountered difficulty with obtaining information and data from DER operators. DER owners should be encouraged to keep their end of any SCADA equipment functional and reconnect their telemetry devices when they have been disabled and this can be done through interconnection requirements. The operator should be alerted by the DER when telemetry is interrupted. Scan rates equivalent to the scan rates used by the system operator are preferred (typically in the 6 second range). Although IEEE 1547-2018 defines and requires a communication port, the path that a utility may use for data from that communication port may pose a cyber-security risk if not adequately secure. It is suggested that full consideration be given to cyber security risks when transferring data until such time as the IEEE 1547 has been amended to require cyber security protections.

Going forward many areas and utilities are either in the process of or determining the value of adding distribution system platforms to deal with DER aggregation, observability, availability and status of DER. NPCC will continue to monitor the development and deployment of these Distributed Energy Resource Monitoring Systems (“DERMS”).

DER Recommendations

As DER continues to proliferate within the NPCC Region we suggest the following initial activities:

Participation in National DER Forums

- 1) Participate in efforts to fully understand the issues and best practices associated with DER.
- 2) Engage NPCC and its members to address the issues and provide expertise.
- 3) As the understanding of the issues and best practices matures, then NPCC will be well positioned to understand the regional differences that need to be considered.

Process and Risk Management Recommendations

- 1) Continue with sensitivity analysis at the Transmission level for various levels of penetration of DER on the distribution facilities to determine effects of increased penetration levels of DER on BPS performance.
- 2) Pursue further opportunities to coordinate distribution and transmission requirements for DER, share Member best practices, and promote consistency regarding DER installations where possible within the NPCC region.
- 3) Continue to review and identify approaches to coordinate NPCC AGIR and utility interconnection requirements relative to DER to identify dissimilarities between Areas which may negatively impact reliability.
- 4) Identify opportunities to share information regarding DER related reliability risk problems and solutions and promote sharing.
- 5) Encourage consideration of developing IT Infrastructure plans to aggregate and report critical DER Status to BPS Operators.
- 6) Continue to solicit and address observable reliability related issues of DER using NPCC's DER Impact Reporting Forms and its associated process.
- 7) Continue to discuss any changes required for System Restoration and Blackstart Plans, as a result of increased DER.
- 8) Continue to follow DER related ESA ESS safety issues and associated recommendations and share the results with NPCC stakeholders.
- 9) Avoid placement of UFLS on distribution feeders which have a significant amount of DER relative to the feeder's load if possible, unless sufficient telemetry exists to ensure proper functionality of the UFLS program as a whole.

Planning Related Recommendations Due to Changing Resource Mix

- 1) Identify and consider new methods to obtain and facilitate collection of DER modeling and performance data to enable Long-Term Resource, Long-Term Transmission and Operational Planning of the BPS¹⁵
- 2) Clearly identify DER in the NPCC Region's Area interconnection queues or forecasts where DER is being proposed for installation, including the magnitude and location relative to the existing resource base and load projections.
- 3) Address masking of load by DER at the distribution level to ascertain its impact on the behavior of load, as well as the assumptions that underpin UFLS programs.
- 4) Determine the appropriate entities responsible for providing DER data to the Planning Coordinator for the purposes of model building and maintenance and ensure that this data is provided.

Analytics and simulation recommendations to deal with increased system complexity

- 1) Support interconnection wide inertia loss study efforts, to determine potential reliability impacts, as DER replaces conventional synchronous generation resources.
- 2) Obtain DER modelling data to be able to model, predict and examine system behavior and assess the interactions between the new resources and the existing reliability preserving systems and programs. Examples include:
 - a. Dynamic behavior of the transmission system
 - b. Sudden loss of large amounts of DER due to transmission system events
 - c. Under Frequency Load Shedding,
 - d. Under Voltage Load Shedding,
 - e. Frequency response sharing mechanisms (BAL standards).
 - f. Analysis of system protection systems (both T and D) so that the parameters to set protection systems and other control systems are known to permit the most reliability benefits to be garnered from the new resources.
- 3) Determine the transmission and distribution benefits and challenges of DER fault-related dynamic voltage support.
- 4) Determine the value to the transmission and distribution systems of the different DER steady-state voltage/reactive power control.

Implementation of IEEE-1547-2018

- 1) Work with the AGIR to assign abnormal performance categories for DER certified as meeting IEEE Std. 1547-2018. For example, synchronous generators could be Category I. All inverter-based generation could be Category III. Exceptions could be allowed for inverter-based technologies that could not meet category III and did not constitute a significant penetration. Exceptions could need to be agreed to by both the distribution and transmission entities.
- 2) Develop standard voltage trip settings (1547-2018 Clause 6.4.1) that provide for BPS reliability. For example for Category III, UV1 could be set at 0.88 p.u. & 3.5 seconds to coordinate with PRC-

¹⁵ Questions exist regarding which entities should be responsible for providing DER data to the Planning Coordinator for the purposes of model building. NERC is working on this issue.

024-2 at 0.88 p.u. & 6 seconds to coordinate with PRC-024-2 with margin for Fault Induced Delayed Voltage Recovery (FIDVR) or at 0.88 p.u. & 10 seconds which conforms with the default setting of Category II I. UV2 could be set at 0.5 p.u. and 2 seconds which conforms with the default setting of Category III.

- 3) Develop standard frequency trip settings (1547-2018 Clause 6.5.1) that provide for BPS reliability. For example, use the default setting which were chosen to coordinate with under frequency load shedding.
- 4) Develop standard frequency droop settings (1547-2018 Clause 6.5.2.7) that provide for BPS reliability. For example, use the default settings that are consist with the requirements for generators connected to the BPS
- 5) Develop standard Enter Service settings (1547-2018 Clause 4.10) that can be used in black start studies. The default delay time is 300 seconds. However, distribution entities may require a shorter delay to reduce the impact of cold load pickup. Also, distribution entities may require different delay times when several large DER are connected to the same feeder
- 6) Develop requirements that ensure protective relay settings on the distribution system coordinate with the voltage and frequency ride-through capabilities established by the selected trip settings. Any exceptions shall be discussed with the transmission provider.

Appendix A, NPCC DER Impact Reporting Form and Process



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

Please Complete and email this form and email to; [npccstandard@npcc.org](mailto:npscstandard@npcc.org)

Distributed Energy Resource (DER), BES Impact Reporting Form

Name		Date	
Email		Company	
Impact on Bulk Electric System		Area (NY, NE, State or Province etc.)	

Equipment Impacted

Equipment	Location (substation name, etc.)	Impact (Positive reliability impact? Negative reliability impact-Protection System failure, Misoperation, load affected or lost?, power quality issue?, etc.)	Duration of Impact, (start and stop times, length of impact, ongoing? etc.)

Description of Impact on BES- What Happened or was observed?

Please describe below the details of all the impacts of the DER as it pertains to this report, such as load loss, loss of life, equipment failure or potential reliability improvement. A sequence of events showing the impact is helpful. Attach supporting information to this form if necessary.

Root Cause or additional Analysis

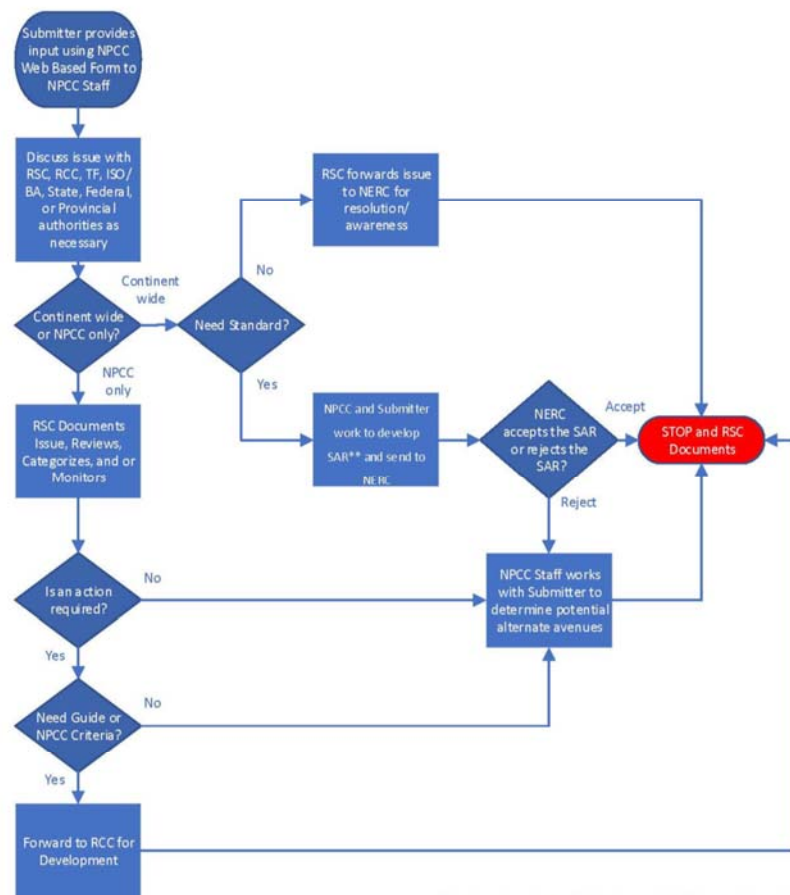
Please describe below the details of any investigation your company may have already done to identify causes or contributing factors to the incident. This will help NPCC route the issue properly to address it.

NPCC Review of Issue and Recommendations (i.e. refer to NERC, develop a Criteria, Guideline, Already Addressed or Identified, etc.)

NPCC Date of Resolution of Issue _____

Evaluation Process

Impacts from Distribution Level* Distributed Energy Resources on the BES



*Distribution Level, Not behind the Meter, utility scale DER

** Standards Authorization Request (SAR)

Regional Standards Committee, Approved 8/22/18 (GVZ)

Appendix B, NPCC Areas- Comparisons

Key Inverter based specification extracts

	ISO-NE Inverter Requirements	NG ESB 756 B, C, D	NY SIR ¹⁶	IESO F2 Technical Requirements
Inverter Certification	yes	yes	yes	yes
Voltage and frequency trip settings for inverter-based applications	yes	yes	yes	yes
Voltage Response	yes ¹⁷	yes	yes	yes
Frequency Response	yes ¹⁸		yes	yes
Abnormal performance capability (ride-through) requirements for inverter-based applications	yes	yes		
Other grid support utility interactive inverter functions statuses	yes			
Minimum protection functions		yes	yes	
Monitoring and Control		yes	yes	yes
Reconnection to the System		yes	yes	
Distribution Protection Coordination		yes		yes
Inverter Certification		yes	yes	
Power Quality			yes	

¹⁶ NY SIR is the [New York Standardized Interconnection Requirement](#).

¹⁷ The functionality is required to be present, but the default state is to have this functionality disabled unless otherwise directed by the area EPS operator

¹⁸ The functionality is required to be present, but the default state is to have this functionality disabled unless otherwise directed by the area EPS operator

Appendix C – SPIDER Working Group Reliability Guidelines & Activities

The NERC System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG) was formed to focus on the impacts that aggregate amounts of DER can have on transmission planning and BPS reliability. This SPIDERWG is seeking to provide high-level, technical recommended practices for ensuring BPS reliability in the face of growing penetrations of DER across North America. The recommended practices and guidance provided by SPIDERWG, in many cases, will need to be adapted to specific utility and regional planning and operating practices. The following DER-related topics are covered, as described in NERC Staff's "Summary of Activities: BPS-Connected Inverter-Based Resources and Distributed Energy Resources"¹⁹:

Modeling: Representing aggregate DER in BPS reliability studies, advancing industry capabilities and expertise with representing DER in these reliability studies, developing robust and reasonable data sets for power flow and dynamic simulations

Verification: Ensuring that the models used in studies provide a reasonable and suitable representation of the actual aggregate performance of these resources, benchmarking software platforms to ensure uniformity in tools, recommending analysis techniques for accounting for aggregate DER during large BPS disturbances

Studies: Improving study techniques and methods to ensure the most stressed operating conditions are chosen for BPS reliability studies, identifying key operating conditions and sensitivities to perform, improving software tools and study capabilities

Coordination: Supporting coordination between transmission and distribution entities for improved data exchange and coordinating with IEEE to support the application of IEEE Std. 1547- 2018 across North America

A list of SPIDERWG Reliability Guidelines and other activities is provided in Table 1 and Table 2, respectively.

¹⁹ Available here: https://www.nerc.com/comm/PC/Documents/Summary_of_Activities_BPS-Connected_IBR_and_DER.pdf

Table 1. SPIDER Working Group Reliability Guidelines

Subgroup	Title	Description	Status
Modeling	DER Data Collection for Modeling	Guideline providing recommended practices for collecting DER data for the purpose of developing aggregate DER models for BPS reliability studies.	In Review – Draft Posted for Comment (here)
	DER_A Model Parameterization	Guideline providing recommendations for using state-of-the-art aggregate DER dynamic models in BPS reliability studies.	Published (here)
Verification	DER Performance and Model Verification	Guideline providing recommended practices for performing model verification for aggregate DER dynamic models including placement of measurement devices, execution of verification simulations, and how to use the data collected through these practices.	In Development
	DER Forecasting Practices and Relationship to DER Modeling for Reliability Studies	Guideline providing how forecasting practices are linked to DER modeling for reliability studies, specifically on how DER are accounted for in future reliability assessments.	In Development
Studies	Bulk Power System Planning under Increasing Penetration of Distributed Energy Resources	Guideline providing recommended practices for performing planning studies considering the impacts of aggregate DER behavior.	In Development
	Recommended Approaches for Developing Underfrequency Load Shedding Programs with Increasing DER Penetration	Guideline regarding how to study UFLS programs and ensure their effectiveness with increasing penetration of DER.	Under Consideration
Coordination	BPS Reliability Perspectives on the Adoption of IEEE 1547-2018	Guideline providing industry recommendations and BPS reliability perspectives on the implementation and adoption of IEEE 1547-2018.	Published (here)
	Communication and Coordination Strategies for Transmission Entities and Distribution Entities regarding Distributed Energy Resources	Guideline recommending strategies to encourage coordination between Transmission and Distribution entities on issues related to DER such as information sharing, performance requirements, DER settings, etc.	In Development

Table 2. SPIDER Working Group Other Activities

Subgroup	Title	Description	Status
Modeling	Modeling Notification: Dispatching DER off Pmax in Case Creation	Notification of accounting for DER in powerflow and dynamics cases, particularly regarding accounting for power output levels with DER utilizing advanced grid-supportive features.	Posted (here)
	DER Modeling Survey	Survey of SPIDERWG member organizations regarding the use of DER models in BPS planning studies.	Compiling Results
Studies	White Paper: Review of TPL-001-5 for Incorporation of DER	White paper discussing technical review of NERC TPL-001-5 in the context of increasing DER and their impacts to the BPS. Possible SAR development following completion of white paper, as needed.	In Review
	White Paper: Recommended Simulation Improvements and Techniques	White Paper recommending simulation software improvements to enhance the ability to accurately account for and model DER.	In Development
	White Paper: DER Impacts to Undervoltage Load Shedding	White Paper briefly discussing how DER may impact UVLS program development.	In Development
	White Paper: Beyond Positive Sequence RMS Simulations for High DER	White Paper highlighting the use of tools that provide additional technical detail to DER studies beyond just positive sequence RMS simulation tools.	In Development
Coordination	Coordination of DER Terminology	Development and ongoing review of definitions and terminology pertaining to DER and related topics.	In Development
	NERC Reliability Standards Review	White Paper reviewing NERC Reliability Standards and the impacts that increasing penetrations DER may have on BPS reliability and standards compliance/implementation. Possible SAR development following completion of white paper, as needed.	In Development
	Tracking and Reporting DER Growth	Coordinated review of information regarding DER growth, including types of DER, size of DER, etc. Consideration for useful tracking techniques for modeling and reliability studies.	In Development

Appendix D, NPCC Reliability Principles

Using its membership structure and governance authority to create and apply Regional Criteria²⁰, NPCC Member adherence to Regional Criteria contributes to a more robust level of reliability beyond NERC ERO reliability “results-based” standards / requirements. For example, NPCC Criteria mandate specific design requirements for NPCC Member facilities. NPCC’s approach to reliability and Resilience can be summarized in Principles that guide NPCC Members in their effort to meet or exceed NERC requirements. NPCC’s core Reliability Principles²¹ and activities support the NERC Bulk Electric System and NPCC’s Bulk Power System reliability.

The NPCC Reliability Principles include:

1. **Focus on the most important system components:** In order to focus resources to those portions of the power delivery system most important (critical) to overall reliability, NPCC Members employ mechanism(s) for identifying those facilities that are most critical to the reliable planning and operation of the power delivery assets in the NPCC region²². These critical facilities collectively are identified as the NPCC Bulk Power System^{23,24}.
2. **Application of Criteria beyond NERC requirements to identified critical facilities:** Where, in the opinion of NPCC’s Membership, the NERC standards do not adequately specify a necessary performance or design outcome in a given technical, operation or planning area, NPCC Criteria govern the design of their respective portions of the NPCC Bulk Power System planning and operation²⁵ activities.
3. **NPCC Members support the Criteria:** NPCC’s Full Members in accordance with the NPCC Bylaws are committed to designing and operating their systems to meet the NPCC Criteria under peer review of the NPCC Full Members.
4. **No conflict with NERC Requirements:** The NPCC Criteria supplement, improve upon where necessary, benefit, and do not conflict with or duplicate the results-based performance

²⁰ See NERC Rule of Procedure #313 on page 15 of the [NERC Rules of Procedure 3-9-2018](#).

²¹ The Reliability Principles were summarized in the NPCC 2018 Strategic Review Report.

²² The method of identifying critical facilities is currently embodied in the [NPCC A-10 Classification of bulk power system Elements](#) document, currently under review by the CP-11 Working Group with a due date of October 31, 2018.

²³ The NPCC bulk power system is identified by a specific list of facilities in the NPCC region deemed critical by the NPCC A-10 classification process. This list is not determined based on the definition of the ERO bulk power system, which is defined in the US 2005 EPACT as:

“(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

“(B) electric energy from generation facilities needed to maintain transmission system reliability.

The term does not include facilities used in the local distribution of electric energy.

²⁴ There are other documents which supplement the Directories, for instance the NPCC Compliance Guidance Statements. These documents usually refer to NERC standards applicability and can be found here: [NPCC CGS](#)

²⁵ NERC [Rule of Procedure](#) #313 (page 15) permits the following: “Regional Entities may develop Regional Criteria that are necessary to implement, to augment, or to comply with NERC Reliability Standards, but which are not Reliability Standards. Regional Criteria may also address issues not within the scope of Reliability Standards, such as resource adequacy. “

requirements of NERC standards where they apply to the NPCC Bulk Power System. NPCC adjusts its Regional Criteria to retire or adapt to any new NERC requirements as they come into effect as necessary.

5. **Include design specifications where needed:** The NPCC Criteria and related guidelines and procedures provide design criteria and practices to assure implementation. NPCC Directories go into greater detail regarding how to accomplish a given reliability result, where NERC standards may simply require a “reliability result.”
6. **Resilience has always been an element of NPCC Criteria:** Based on experience, resilience^{26 27} is a necessary constituent component of reliability and it is important both to electricity consumers and regulatory authorities in NPCC’s Region. NPCC Criteria provide substantial resilience benefits to the NPCC Bulk Power System by providing:
 - a. Robustness – The ability to withstand disturbances by supporting operations in a more secure state.
 - b. Resourcefulness – The ability to detect and manage a crisis as it unfolds.
 - c. Rapid recovery – The ability to get services back as quickly as possible in a coordinated and controlled manner.
 - d. Adaptability – The ability to absorb new lessons from events

²⁶ Reference NERC’s recent [filing](#) with FERC regarding Resilience for a more complete discussion of the relationship between resilience, the NERC standards and the NAICS Resilience Framework. FERC is expected to define resilience in the course of its current examination of electric system resilience concepts.

²⁷In the US, [Presidential Policy Directive – 21](#) defines resilience as “The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents”.

NERC, Model of Resilience

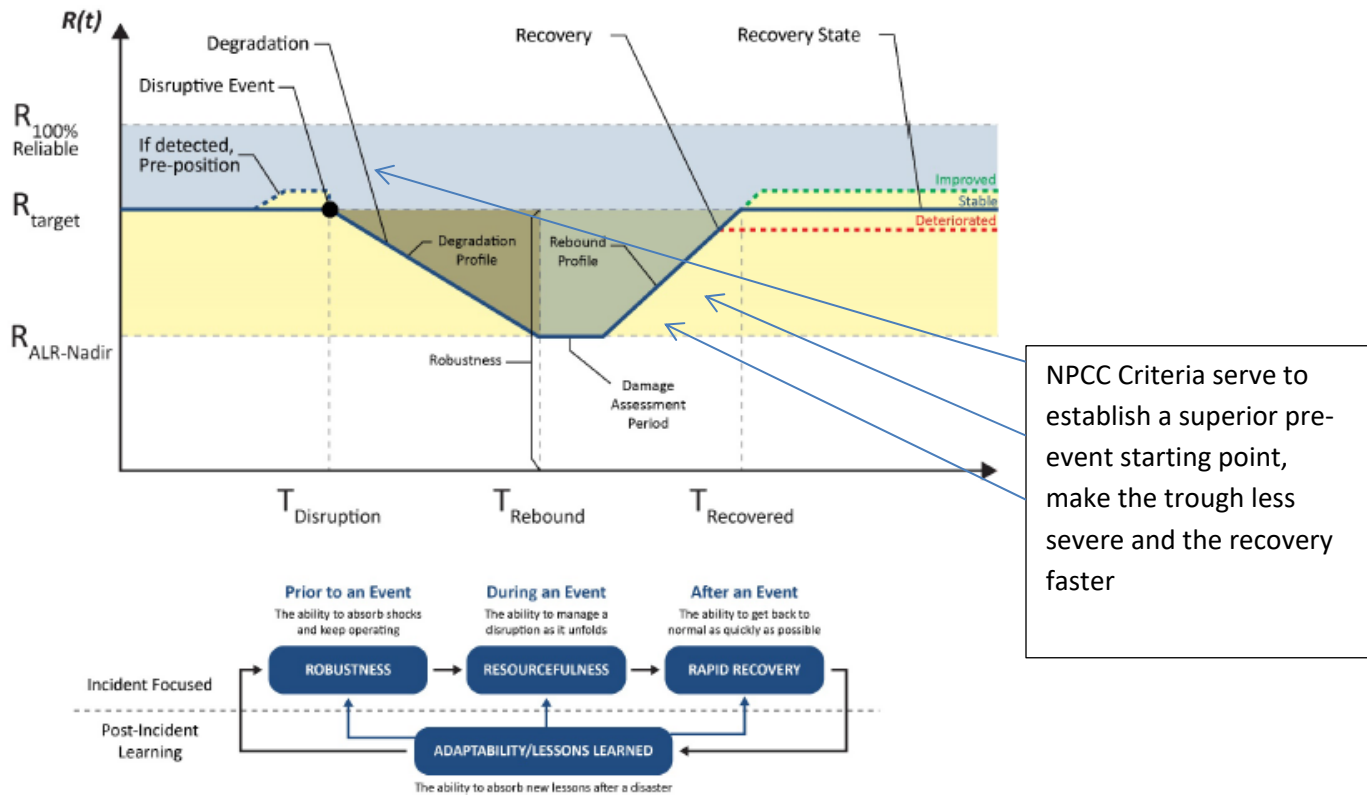


Figure 2.1

Figure 2.1 depicts a typical disruptive event and maps how the systems responds in a qualitative fashion. The y-axis above is meant to represent a relative level of reliability and system response is plotted temporally. DER will increasingly fill a critical role with respect to reliability and Resilience of the Bulk Electric System. Specifically, DER can contribute to the overall robustness of the system and provide increased resource support within islands during system separations. As DER continues to penetrate the system, changes to NPCC's Underfrequency Load Shedding program may be required.

Appendix E, State and Provincial AGIR Information

New York State

Statewide Interconnection Technical Documents may be found at:

[Interconnection Technical Working Group Webpage](#)

New England, by State

Inverter Source Requirement Document of ISO New England (ISO-NE)

Connecticut –

Department of Energy and Environmental Protection, Public Utilities Regulatory Authority (PURA)

Eversource Energy – Connecticut Interconnection Standard

<https://www.eversource.com/content/general/about/about-us/doing-business-with-us/builders-contractors/interconnections/connecticut-application-to-connect>

Summary of Facility Connection Requirements for Generation, Transmission and End Users Connecting to UI Transmission Facilities, Revision 4.0, December 7, 2015:

<https://www.uinet.com/wps/wcm/connect/89138d72-c4a0-403b-9871-937a00f91c42/NERC%2BFAC-001%2BInterconnect%2Bsummary%2BDocument%2BRevision%2B4.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-89138d72-c4a0-403b-9871-937a00f91c42-mkr0qCb>

Eversource/United Illuminating Guidelines for Generator Interconnection, Fast Track and Study Processes, April 5, 2019:

https://www.uinet.com/wps/wcm/connect/bd802aec-1e83-4051-8a6e-58f0cb98d1fd/Guideline_for_Generator_Interconnection_Fast_Track_and_Study_Process_5-12-10_doc_1577.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-bd802aec-1e83-4051-8a6e-58f0cb98d1fd-miUZQ4n

Maine –

Maine Public Utilities Commission

Chapter 324 Small Generator Interconnection Procedures

Central Maine Power Transmission and Distribution Interconnection Requirements for Generation, December 15, 2018:

<https://www.cmpco.com/wps/wcm/connect/dee5fbf1-7af0-40ec-b06c-af3ec015e0be/SchB-TransmissionDistributionInterconnectionRequirementsforGeneration.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-dee5fbf1-7af0-40ec-b06c-af3ec015e0be-mwfmMCK>

Emera Maine Interconnection Agreement:

<https://www.emeramaine.com/energy-solutions/connecting-renewable-resources/small-generator-interconnection-process/>

Massachusetts –

MA Department of Public Utilities (MADPU) interim guidance (DPU 19-55)

MADPU Massachusetts Department of Energy Resources

MADPU Interconnecting Renewable Energy webpages with links to: resources, past and present proceedings before the DPU, each electric distribution companies' tariff, and the Ombudsperson dispute resolution process: <https://www.mass.gov/interconnecting-renewable-energy-facilities>

MADPU is currently conducting a large-scale investigation into the rules and procedures by which distributed generation is interconnected in Massachusetts in docket D.P.U. 19-55. This investigation includes implementation of IEEE 1547-2018. Documents and information can be found in our online file room: <https://eeaonline.eea.state.ma.us/DPU/Fileroom/dockets/bynumber> (enter "19-55")

Massachusetts Technical Standards Review Group:
<https://sites.google.com/site/massdgic/home/interconnection/technical-standards-review-group>

Renewable energy generally: <https://www.mass.gov/topics/renewable-energy>

MADPU Net Metering Information: <https://www.mass.gov/net-metering>

MADOER SMART Program Information: <https://www.mass.gov/info-details/solar-massachusetts-renewable-target-smart-program>

Who to contact in MA for your renewable energy question: <https://www.mass.gov/info-details/who-to-contact-about-my-renewable-energy-question-or-concern>

Massachusetts Utilities

National Grid / Supplement to Specifications for Electrical Installations / ESB 756-2019 ver. 5.0 (Section 7.8 includes voltage and frequency ride through and control requirements);

https://www9.nationalgridus.com/non_html/shared_constr_esb756.pdf

NSTAR ELECTRIC COMPANY d/b/a EVERSOURCE ENERGY STANDARDS FOR INTERCONNECTION OF DISTRIBUTED GENERATION, M.D.P.U. No. 55, Effective: February 1, 2018:

https://author.eversource.com/content/docs/default-source/rates-tariffs/ma-electric/55-tariff-ma.pdf?sfvrsn=8582c462_6

Unitil Energy Systems, Inc. Interconnection Standards for Inverters Sized up to 100 kVA:

https://unitil.com/sites/default/files/pdfs/UES%20100%20KVA%20Interconnect%20Standard%202009_08_21_1.pdf

Individual Massachusetts Municipal Electric Utility Entity Interconnection Requirements:

<https://www.mass.gov/guides/net-metering-guide>

New Hampshire –

New Hampshire Public Utilities Commission

Liberty Utilities Electricity Delivery Service Tariff – NHPUC No. 20:

https://www.puc.nh.gov/Regulatory/Docketbk/2018/18-183/INITIAL%20FILING%20-%20PETITION/18-183_2018-12-10_GSEC_TARIFF.PDF

New Hampshire Electric Co-op Net Metering Requirements:

<https://www.nhec.com/wp-content/uploads/2017/02/2017-Interconnection-Application-Package.pdf>

Public Service Company of New Hampshire Interconnection Standards for Inverters Sized Up to 100 KVA, August 2009:

https://www.eversource.com/content/docs/default-source/builders-contractors/eversource's-interconnection-standards-for-inverters.pdf?sfvrsn=2dd9cf62_0

Unitil Energy Systems, Inc. Interconnection Standards for Inverters Sized up to 100 kVA:

https://unitil.com/sites/default/files/pdfs/UES%20100%20KVA%20Interconnect%20Standard%202009_08_21_1.pdf

Rhode Island –

State of Rhode Island Public Utilities Commission and Division of Public Utilities and Carriers

Block Island Power Company Net Metering Application:

<https://blockislandpowercompany.com/net-metering-application-2/>

The Narragansett Electric Company Standards for Connecting Distributed Generation, Effective September 6, 2018:

https://www9.nationalgridus.com/non_html/RI_DG_Interconnection_Tariff.pdf

Pascoag Utility District – Electric Net Metering Policy, Requested Effective Date: June 1, 2010:

<https://www.pud-ri.org/wp-content9999/uploads/2015/07/Net-Metering-Policy.pdf>

Vermont –

Vermont Public Utility Commission

The Vermont Public Utility Commission issued an interconnection rule in 2006 that was largely modeled on the FERC Small Generator Interconnection Procedures at that time. The rule has not been updated since 2006.

Links to the current rule as well as an application form and application instructions:

PUC Rule 5.500 – Interconnection Rule

https://puc.vermont.gov/sites/psbnew/files/doc_library/5500-electric-generation-interconnection-procedures_0.pdf

PUC Rule 5.500 – Application Form

https://puc.vermont.gov/sites/psbnew/files/doc_library/5500-revised-application_0.pdf

PUC Rule 5.500 – Application Instructions

https://puc.vermont.gov/sites/psbnew/files/doc_library/5500-revised-application-instructions_0.pdf

In addition, the Department petitioned the PUC to initiate a rulemaking to make adjustments to the interconnection rule in 2016. As of the date of this DER Guidance document there were some filings and a workshop, but the process recently ended without resolution. The PUC has indicated that they are likely to take up the process again in the near future however has not provided NPCC with a date. Information regarding this process can be found here: <https://puc.vermont.gov/about-us/statutes-and-rules/proposed-changes-rule-5500>

Province of Quebec (some references are only available in French)

Section 112 of the [Act respecting the Régie de l'énergie](#) (chapter R-6.01) (the Act) reads as follows:

112. THE GOVERNMENT MAY MAKE REGULATIONS DETERMINING

[...]

(2.1) *for a particular source of electric power supply, the corresponding energy block and maximum price established for the purpose of fixing the cost of electric power referred to in section 52.2 or for the purposes of the supply plan provided for in section 72, or for the purposes of a tender solicitation by the electric power distributor under section 74.1;*

(2.2) *the timeframe applicable to a public tender solicitation by the electric power distributor under section 74.1;*

(2.3) *the maximum production capacity referred to in section 74.3, which may vary with the source of renewable energy or the class of customers or producers specified;*

[...]

In cases where energy needs are to be supplied out of an energy block, a regulation may provide that only certain classes of suppliers may be invited to tender by the electric power distributor and that the quantity of electric power required under each supply contract may be limited.

Consequently, the Government has taken the following regulations, regarding Distributed Energy Resources (or DER), between 2003 and 2013:

- [CONCERNANT le Règlement sur l'énergie produite par cogénération](#) (Décret 1319-2003, 10 décembre 2003);
- [CONCERNANT le Règlement sur l'énergie éolienne et sur l'énergie produite avec de la biomasse](#) (Décret 352-2003, 5 mars 2003);
- [CONCERNANT le Règlement modifiant le Règlement sur l'énergie produite par cogénération](#) (Décret 298-2004, 29 mars 2004);
- [CONCERNANT le Règlement sur le second bloc d'énergie éolienne](#) (Décret 926-2005, 12 octobre 2005);
- [CONCERNANT le Règlement sur l'énergie produite par cogénération à la biomasse](#) (Décret 916-2008, 24 septembre 2008);
- [CONCERNANT le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 1043-2008, 29 octobre 2009);
- [CONCERNANT le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 1045-2008, 29 octobre 2008);
- [CONCERNANT le Règlement modifiant le Règlement sur l'énergie produite par cogénération à la biomasse](#) (Décret 9-2009, 7 janvier 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 179-2009, 4 mars 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 180-2009, 4 mars 2009);
- [CONCERNANT le Règlement sur la capacité maximale de production visée dans un programme d'achat d'électricité pour des petites centrales hydroélectriques](#) (Décret 336-2009, 25 mars 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 520-2009, 29 avril 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 521-2009, 29 avril 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 468-2010, 2 juin 2010);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 469-2010, 2 juin 2010);
- [CONCERNANT le Règlement sur la capacité maximale de production visée dans un programme d'achat d'électricité produite par cogénération à base de biomasse forestière résiduelle](#) (Décret 1085-2011, 26 octobre 2011);
- [CONCERNANT le Règlement sur un bloc de 450 mégawatts d'énergie éolienne](#) (Décret 1149-2013, 6 novembre 2013).

The following regulations, or modified regulations (marked in yellow highlight in the section above) have led to four tender solicitations, targeting precise quantities, or energy blocks, of wind Energy:

- [CONCERNANT le Règlement sur l'énergie éolienne et sur l'énergie produite avec de la biomasse](#) (Décret 352-2003, 5 mars 2003);

- [CONCERNANT le Règlement sur le second bloc d'énergie éolienne](#) (Décret 926-2005, 12 octobre 2005);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 468-2010, 2 juin 2010);
- [CONCERNANT le Règlement sur un bloc de 450 mégawatts d'énergie éolienne](#) (Décret 1149-2013, 6 novembre 2013).

The Régie considers the results of these tenders when examining Hydro-Québec's supply plan, as per section 72 of the Act:

***72.** With the exception of private electric power systems, a holder of exclusive electric power or natural gas distribution rights shall prepare and submit to the Régie for approval, according to the form, tenor and intervals fixed by regulation of the Régie, a supply plan describing the characteristics of the contracts the holder intends to enter into in order to meet the needs of Québec markets following the implementation of the energy efficiency measures. The supply plan shall be prepared having regard to*

- (1) the risks inherent in the sources of supply chosen by the holder;*
- (2) as concerns any particular source of electric power, the energy block established by regulation of the Government under subparagraph 2.1 of the first paragraph of section 112; and*

[...]

When examining a supply plan for approval, the Régie shall consider such economic, social and environmental concerns as have been identified by order by the Government.

Sections 74.1 and 74.2 of the Act provide that the Régie oversees the process of such tender solicitations:

***74.1.** To ensure that suppliers responding to a tender solicitation are treated with fairness and impartiality, the electric power distributor shall establish and submit for approval to the Régie, which shall make its decision within 90 days, a tender solicitation and contract awarding procedure and a tender solicitation code of ethics applicable to the electric power supply contracts required to meet the needs of Québec markets in excess of the heritage pool, or the needs to be supplied out of an energy block determined by regulation of the Government under subparagraph 2.1 of the first paragraph of section 112.*

The tender solicitation and contract awarding procedure shall, in particular,

- (1) allow all interested suppliers to tender by requiring the tender solicitation to be issued in due time;*
- (2) grant equal treatment to all sources of supply and energy efficiency projects unless the tender specifications provide that all or part of the needs met by a particular source of supply must be supplied out of an energy block determined by regulation of the Government;*
- (3) favour the awarding of supply contracts based on the lowest tendered price for the required quantity of electric power and in keeping with the required conditions, taking into account the applicable transmission cost and, where the tender specifications provide that all or part of the needs met by a particular source of supply must be supplied out of an energy block, taking into account the maximum price established by regulation of the Government; and*
- (4) provide that, following a tender solicitation, contracts may be awarded to two or more suppliers, in which case a supplier offering the required quantity of electric power may be invited to reduce the quantity offered without modifying the tendered unit price.*

An energy efficiency project to which a tender solicitation applies under subparagraph 2 of the second paragraph must meet the stability, sustainability and reliability requirements that apply to conventional sources of supply.

The Régie may dispense the electric power distributor from soliciting tenders for short-term contracts or where urgent needs must be met.

For the purposes of this section, the promoter of an energy efficiency project is deemed to be an electric power supplier.

74.2. *The Régie shall monitor the implementation of the tender solicitation and contract awarding procedure and code of ethics provided for in section 74.1 and ascertain whether they are complied with. To that end, the Régie may require any document or information it considers useful. The Régie shall report its findings to the electric power distributor and to the supplier chosen.*

The electric power distributor may not enter into an electric power supply contract unless it has obtained the approval of the Régie, under the conditions and in the cases determined by regulation by the Régie.

The Régie's Website lists every docket related to this jurisdiction over Québec's electricity distributor (in French only): [Approval of supply contracts](#).

The Régie also considers DER when adopting specific reliability standards. Sections 85.2 and 85.7 of the Act read as follows:

85.2. *The Régie shall ensure that electric power transmission in Québec is carried out according to the reliability standards it adopts.*

85.7. *The Régie may request the reliability coordinator to modify a standard filed or submit a new one, on the conditions it sets. It shall adopt reliability standards and set the date of their coming into force.*

The reliability standards may

- (1) subject to section 85.10, provide for a schedule of sanctions, including financial penalties, that apply if standards are not complied with; and*
- (2) refer to reliability standards set by a standardization agency that has entered into an agreement.*

Docket [R-4070-2018](#) (in French only) relates to a request by the reliability coordinator (HQCME) and is still under examination by the Régie. It aims the adoption of reliability standards associated with Special Protection System (Remedial Action Scheme) and Dispersed Power Producing Resources.

The following sections of Québec' electricity distributor and transmitter's web site might be useful, since they list the applicable technical codes, standards and requirements:

- http://www.hydroquebec.com/transenergie/fr/commerce/raccordement_distribution.html ;
- http://www.hydroquebec.com/transenergie/fr/commerce/raccordement_transport.html

Province of Ontario

The current connection requirements for all resources can be found in Chapter 4 appendices 4.2 and 4.3 of the Market Rules. <http://www.ieso.ca/-/media/Files/IESO/Document-Library/Market-Rules-and-Manuals-Library/market-rules/mr-chapter4appx.pdf?la=en>

The Independent Electric System Operator (IESO) is in the process of making updates to these requirements to be more specific about the requirements that apply to all DERs (not just storage). <http://www.ieso.ca/Sector-Participants/Engagement-Initiatives/Engagements/Updates-to-Performance-Requirements-Market-Rule-Appendices-4-2-and-4-3>

The IESO is working on several white papers. The one that was posted in 2019 called “**Exploring Expanded DER Participation in the IESO-Administered Markets**” sets out the participation models that exist for DER in wholesale markets in general and in the IESO-Administered Markets (IAM) today and

also identify the range of options that exist for expanded participation in the future. In addition, this paper provides a working definition of DER, sets out principles for integrating them into wholesale markets, offers an initial review of participation models in other jurisdictions, and identifies key barriers that may limit DER participation in the IAMs.

<http://www.ieso.ca/-/media/Files/IESO/Document-Library/White-papers/White-paper-series-Conceptual-Models-for-DER-Participation.pdf?la=en>

The Ontario Energy Board is also engaging in several stakeholder activities in this area. Below are the links to those activities. The Ontario Energy Board has combined the first two initiatives into one engagement.

1. **Responding to Distributed Energy Resources (DER)*** - The purpose of this initiative is to develop a more comprehensive regulatory framework that facilitates investment and operation of DER based-on value to consumers and supports effective DER integration so the benefits of sector evolution can be realized.

<https://www.oeb.ca/industry/policy-initiatives-and-consultations/responding-distributed-energy-resources-ders>

2. **Utility Remuneration*** - The purpose of this initiative is to identify how to remunerate utilities in ways that make them indifferent to traditional or innovative solutions, better supports their pursuit of least cost solutions, strengthens their focus on long-term value and requires them to reflect the impact of sector evolution in their system planning and operations.

<https://www.oeb.ca/industry/policy-initiatives-and-consultations/utility-remuneration>

3. **DER Connections Review** – The purpose of this initiative to review its requirements regarding the connection of distributed energy resources (DER) by licensed electricity distributors. The purpose of this initiative is to identify any barriers to the connection of DER, and where appropriate to standardize and improve the connection process. The review will be focused on connection of electricity generation and storage facilities connected to the distribution system, either in front or behind the distributor's meter.

<https://www.oeb.ca/industry/policy-initiatives-and-consultations/distributed-energy-resources-der-connections-review>

The contact for this information would be Customer Relations (customer.relations@ieso.ca)

Province of New Brunswick

Within the province, DER is referred to as “Embedded Generation” or “Distributed Generation.” Regulation from the New Brunswick Energy and Utility Board may be found here:

<http://laws.gnb.ca/en/ShowPdf/cs/2013-c.7.pdf>

Énergie NB Power’s embedded generation may be found here:

<https://www.nbpower.com/en/products-services/embedded-generation/>

Appendix F, ISO New England

ISO-NE specific Inverter requirements are as follows in the below table and the link

[Inverter Source Requirement Document of ISO New England](#)

The following additional performance requirements are applied in one NPCC Area and are provided as an example:

- In the Permissive Operation region above 0.5 p.u., inverters shall ride-through in Mandatory Operation mode, and
- In the Permissive Operation region below 0.5 p.u., inverters shall ride-through in Momentary Cessation mode.

Table I: Inverters' Voltage Trip Settings

Shall Trip – IEEE Std 1547-2018 (2 nd ed.) Category II					
Shall Trip Function	Required Settings		Comparison to IEEE Std 1547-2018 (2 nd ed.) default settings and ranges of allowable settings for Category II		
	Voltage (p.u. of nominal voltage)	Clearing Time(s)	Voltage	Clearing Time(s)	Within ranges of allowable settings?
OV2	1.20	0.16	Identical	Identical	Yes
OV1	1.10	2.0	Identical	Identical	Yes
UV1	0.88	2.0	Higher (default is 0.70 p.u.)	Much shorter (default is 10 s)	Yes
UV2	0.50	1.1	Slightly higher (default is 0.45 p.u.)	Much longer (default is 0.16 s)	Yes

Table II: Inverters' Frequency Trip Settings

Shall Trip Function	Required Settings		Comparison to IEEE Std 1547-2018 (2 nd ed.) default settings and ranges of allowable settings for Category I, Category II, and Category III		
	Frequency (Hz)	Clearing Time(s)	Frequency	Clearing Time(s)	Within ranges of allowable settings?
OF2	62.0	0.16	Identical	Identical	Yes
OF1	61.2	300.0	Identical	Identical	Yes
UF1	58.5	300.0	Identical	Identical	Yes
UF2	56.5	0.16	Identical	Identical	Yes

Table III: Inverters' Voltage Ride-through Capability and Operational Requirements

Voltage Range (p.u.)	Operating Mode/ Response	Minimum Ride-through Time(s) (design criteria)	Maximum Response Time(s) (design criteria)	Comparison to IEEE Std 1547-2018 (2 nd ed.) for Category II
$V > 1.20$	Cease to Energize	N/A	0.16	Identical
$1.175 < V \leq 1.20$	Permissive Operation	0.2	N/A	Identical
$1.15 < V \leq 1.175$	Permissive Operation	0.5	N/A	Identical
$1.10 < V \leq 1.15$	Permissive Operation	1	N/A	Identical

$0.88 \leq V \leq 1.10$	Continuous Operation	infinite	N/A	Identical
$0.65 \leq V < 0.88$	Mandatory Operation	Linear slope of 8.7 s/1 p.u. voltage starting at 3 s @ 0.65 p.u.: $T = 3 \text{ s} + \frac{8.7 \text{ s}}{V - 0.65 \text{ p.u.}}$ VRT 1 p. u.	N/A	Identical
$0.45 \leq V < 0.65$	Permissive Operation ^{a,b}	0.32	N/A	See footnotes a & b
$0.30 \leq V < 0.45$	Permissive Operation ^b	0.16	N/A	See footnote b
$V < 0.30$	Cease to Energize	N/A	0.16	Identical

The following additional operational requirements can be used. Provided as an example:

- In the Permissive Operation region above 0.5 p.u., inverters shall ride-through in Mandatory Operation mode, and
- In the Permissive Operation region below 0.5 p.u., inverters shall ride-through in Momentary Cessation mode with a maximum response time of 0.083 seconds.

Table IV: Inverters' Frequency Ride-through Capability

Frequency Range (Hz)	Operating Mode	Minimum Time(s) (design criteria)	Comparison to IEEE Std 1547-2018 (2 nd ed.) for Category II
$f > 62.0$	No ride-through requirements apply to this range		Identical
$61.2 < f \leq 61.8$	Mandatory Operation	299	Identical
$58.8 \leq f \leq 61.2$	Continuous Operation	Infinite	Identical
$57.0 \leq f < 58.8$	Mandatory Operation	299	Identical
$f < 57.0$	No ride-through requirements apply to this range		Identical

Table V: Grid Support Utility Interactive Inverter Functions Status

Function	Default Activation State
SPF, Specified Power Factor	OFF ²
Q(V), Volt-Var Function with Watt or Var Priority	OFF Default value: 2% of maximum current output per second
SS, Soft-Start Ramp Rate	ON
FW, Freq-Watt Function OFF	OFF

Appendix G, State Renewable and Green Energy Targets

New York State

70% renewable energy by 2030
85% reduction of Greenhouse Gas emissions by 2050
6,000 MW of distributed solar by 2025
3,000 MW of energy storage by 2025
Carbon free electricity system by 2040

Connecticut

Carbon free electricity system by 2040
Renewable Portfolio Standard - <https://portal.ct.gov/PURA/RPS/Renewable-Portfolio-Standards-Overview>

Vermont

90% of Vermont's overall energy needs from renewable sources by 2050
Reduce Vermont's greenhouse gas (GHG) emissions by 50% from the 1990 baseline level by 2028, and by 75% from the 1990 level by 2050

New Hampshire

20% to 25% reduction in Greenhouse Gas emissions by 2032
25.2% renewable energy by 2025

Rhode Island

100% renewable energy by 2030
1,000 MW of new clean energy installed in 2020

Maine

80% renewable energy by 2030

Appendix H, Autonomous Energy Grids

The National Renewable Energy Laboratory (NREL) and its partners are conducting research and development of advanced techniques that would enable the optimization and control of hundreds of millions of deployed distributed energy resources (DER). The concept known as “Autonomous Energy Grids (AEGs)” are multi-layer, or hierarchical, cellular-structured power grid and control systems that enable resilient, reliability, and economic optimization²⁸. Supported by a scalable, reconfigurable, and self-organizing information and control infrastructure, AEGs are extremely secure and resilient, and can operate in real time to ensure economic and reliable performance while systematically integrating energy in all forms. AEGs rely on cellular building blocks that can self-optimize when isolated from a larger grid and participate in optimal operation when interconnected to a larger grid. The figure H-1 shows how a scalable approach to control can be built from the lowest level of individual controllable technologies (renewable energy, conventional generation, electric vehicles, storage, and loads) and used to control hundreds of millions of devices through the use of hierarchical cells. To make this idea a reality, there are control algorithms for AEGs that will need to be developed and implemented with the following characteristics:

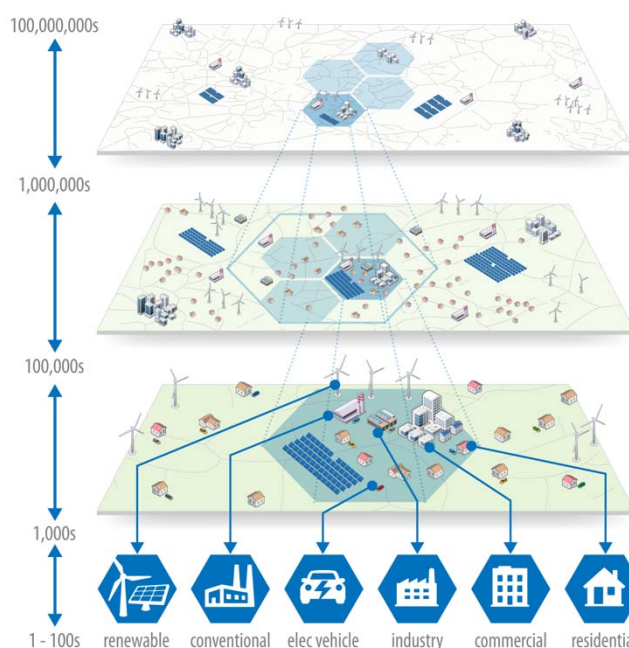


Figure H-1: Autonomous Energy Grids form a distributed hierarchical control system that integrated individual technologies in a cellular structure to the bulk power system.

- **Operate in Real Time** – Control algorithms must operate fast enough to ensure real-time operations in power grids that balance load and generation every second.
- **Handle Asynchronous Data and Control Actions** – Data needs to be used from a variety of asynchronous measurements and sources; whereas distributed decision-making leads to asynchronous control actions.
- **Robustness** – This covers both reliability and resilience, where reliability is fault tolerance and resilience are the ability to come back from a failed state. These control systems must also be

²⁸ “Autonomous Energy Grids”, B. Kroposki, E. Dall’Anese, A. Bernstein, Y. Zhang, B. Hodge, Proceedings of the 51st Hawaii International Conference on System Sciences, January 2018, <https://scholarspace.manoa.hawaii.edu/bitstream/10125/50229/1/paper0342.pdf>

robust to communications failures, prolonged communications outages, and large-scale disturbances.

- **Scalable**— Control algorithms must operate in a scalable fashion to ensure control of hundreds of millions of devices.

NREL has evaluated the AEG algorithms on both large-scale laboratory testing and small-scale real-world demonstrations. NREL evaluated the algorithms as part of the DOE ARPA-E NODES program that demonstrated the first implementation of the algorithms in hardware and successfully demonstrate real-time optimization of a single AEG cell with more than 100 controllable devices at NREL's Energy Systems Integration Facility²⁹. The experiment includes simulation of a real distribution feeder from California with 366 single-phase connection points, more than 100 controllable assets at power (inverters, electric vehicles, and batteries), and hundreds of simulated devices. The distributed algorithms were implemented in cost-effective microcontrollers that self-optimize and communicate to the central coordinator to attain system-wide goals (voltage regulation, frequency response).

NREL has also moved out of the lab to demonstrate the deployment of AEGs in the real world. The team has been working with Holy Cross Energy (HCE), a utility cooperative near Aspen, Colorado, to deploy the AEG technology in a group of smart homes in Basalt, CO³⁰. The smart homes in Basalt Vista are a pilot for an altogether new approach to the grid. These homes optimize energy for residents and their neighbors, but the principles behind Basalt Vista go much further. Within homes, each new connected device or energy resource like a residential battery, water heater, or solar photovoltaic (PV) system, can be controlled for unprecedented energy efficiency. And at a larger scale, entire communities could rapidly share power, creating reliable energy for everyone.

²⁹ <https://www.nrel.gov/news/features/2019/from-the-bottom-up-designing-a-decentralized-power-system.html>

³⁰ <https://www.nrel.gov/news/features/2019/small-colorado-utility-sets-national-renewable-electricity-example-using-nrel-algorithms.html>



Recent FERC Activities

Kal Ayoub

Deputy Director, Division of Cyber Security, Office of Electric Reliability

Federal Energy Regulatory Commission

February 10, 2021

The views expressed in this presentation are my own and do not represent those of the Commission or any individual Commissioner

Recent FERC Orders / NOPRs

WECC Regional Reliability Standard BAL-002-WECC-3 (Contingency Reserve), Docket No. RM19-20-000.

On 10/15/20, the Commission issued a NOPR proposing to approve the proposed Regional Reliability Standard and directed NERC and WECC to submit an informational filing 27 months following its implementation.

Business Plans and Budgets, Docket No. RR20-6-000.

On 11/2/20, the Commission issued an order approving the 2021 budgets of NERC, Regional Entities, and WIRAB.

NPCC SPM, Docket No. RR20-7-000.

On 11/23/20, the Commission issued a letter order approving revisions to NPCC Standard Process Manual.

Recent FERC Orders / NOPRs

Reliability Standard PRC-006-5 (Automatic Underfrequency Load Shedding), Docket No. RD21-1-000.

On 12/23/20, the Commission issued a letter order approving proposed Reliability Standard PRC-006-5.

Reliability Standard PRC-006-5 includes revisions to the WECC regional Variance that clarify applicability of continent-wide requirements to entities in the Western Interconnection and clarify the applicability of the WECC regional Variance to Planning Coordinators.

Delegation Agreements, Docket No. RR20-5-000.

- On 12/30/20, the Commission issued an order conditionally approving the revised *pro forma* Delegation Agreement and the revised Delegation Agreements between NERC and each of the six Regional Entities.
- The order directed NERC and the Regional Entities to modify the revised Delegation Agreements within 120 days of order. The order noted that if a Regional Entity modifies its selection of a hearing process, NERC and the Regional Entities will amend the Delegation Agreements and file such amendments with the Commission.

Virtualization, Cloud Services for Power Grid Operations

- On 12/17/20, the Commission issued an order directing NERC to make an informational filing that considers the feasibility of modifying the CIP Reliability Standards to facilitate the voluntary use of virtualization and cloud computing for purposes beyond data storage (i.e., to perform BES reliability operating services), as well as the status and schedule for any plans to modify the standards by NERC in response to comments filed in response to the 2/20/20 NOI. Docket No. RM20-8.
- The order stated that the Commission supports NERC's effort to reassess the CIP Reliability Standards to facilitate the adoption of virtualization and cloud computing and relieving registered entities of compliance uncertainties. However, consistent with the precept that the Reliability Standards are technology-neutral, virtualization and cloud computing should continue to be voluntary to allow registered entities to consider the deployment of these new technologies, their system needs, and applicable security requirements.
- The Order directed NERC to make the filing by 1/1/22.

Transmission Cyber Security Incentives NOPR

- Issued December 17, 2020, Docket No. RM21-3-000.
- The Commission is proposing under sections 205 and 206 of the Federal Power Act (FPA) to establish rules for incentive-based rate treatments for voluntary cybersecurity investments by a public utility.
- These rules would provide cybersecurity incentives to public utilities that make certain cybersecurity investments that go above and beyond the requirements of the CIP Reliability Standards, and materially enhance the cybersecurity posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards, to the benefit of ratepayers.
- Initial comments due 4/6/2021, reply comments due 5/6/2021.

ERO Five-Year Performance Assessment

- On 1/19/21, the Commission issued an order approving NERC's proposed modifications to its Rules of Procedure related to: (1) the E-ISAC (section 1003); (2) Sanction Guidelines (Appendix 4B); and (3) Registration and Certification (section 500 and Appendices 2, 5A, 5B, and 5C), Docket No. RR19-7-001.
- The order denies NERC's proposal to replace its Appendix 4A audit process with an alternative program and directs NERC to submit completed reports on its audits of all six Regional Entities by June 30, 2023.
- The order accepts NERC's description of its Reliability Guidelines process and its explanation on E-ISAC operations and its All Points Bulletins (APBs) issuances.
- The order directs NERC to submit a further compliance filing within 120 days of this order that: (1) further clarifies information sharing between NERC and the E-ISAC, including the gap analysis process that is currently under development; and (2) revises its Rules of Procedure to explicitly require that NERC must share all APBs with the Commission no later than at the time of issuance.

Revisions to Regulations on ERO Performance Assessments

- On 1/19/21, the Commission issued a NOPR proposing to revise its regulations on the ERO's Performance Assessments, Docket No. RM21-12.
- The NOPR proposes to modify the Commission's regulations on the ERO requirement to submit a performance assessment from the current five-year cycle to a submission every three years.
- The NOPR also proposes to add a requirement for the ERO to include in its performance assessment a detailed discussion of any areas of the ERO's responsibilities and activities, or a Regional Entity's delegated functions, beyond those required by the Commission's regulations, that the Commission has identified at least 90 days prior to the expected performance assessment submission date.
- Finally, the NOPR proposes formalizing the method for the ERO and REs to receive and respond to recommendations by the users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the ERO's operations, activities, oversight and procedures.
- Comments are due 30 days after filing posting in the Federal Register.

- Thank you!
- Questions?



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

NPCC 2021 Corporate Reliability Goals Board Accepted 1-27-2021

NPCC is committed to the **vision of a highly reliable and secure North American bulk power system (BPS)**. NPCC's specific role in support of the overall ERO Enterprise mission is to assure the effective and efficient reduction of risks to the reliability, resilience, and security of the international BPS within Northeastern North America. NPCC works collaboratively with NERC and the other Regional Entities to collectively attain the reliability objectives identified in the *ERO Enterprise Long term Strategy*.

To facilitate NPCC's implementation alignment with the ERO Enterprise Long term Strategy's key focus areas, the Board has established a *Working Draft Strategic Plan* that looks ahead three years to successfully position NPCC, as an international Regional Entity, to be able to respond to anticipated structural changes in the electricity industry, growing reliability interdependencies, and evolving challenges and opportunities that will require NPCC to adapt how it achieves its reliability objectives in the future. The Strategic Reliability Focus Areas for the NPCC 2021 – 2024 *Working Draft Strategic Plan* include: Enhancing System Resilience and Assuring Energy Sufficiency; Reliably Integrating the Resources brought forward by Societal De-carbonization Objectives, including Variable Energy Resources ("VER"), Distributed Energy Resources ("DER"), energy storage, etc.; and Addressing Cyber and Physical Threats. Also included in the *Working Draft Strategic Plan* are a number of tactical initiatives intended to ensure that NPCC's planning, resources, budget, and reliability assurance efforts align with and add value to its stakeholders and the ERO Enterprise.

Each of the NPCC 2021 Corporate Goals is presented in terms of support of a Strategic Focus Area within the *Working Draft Strategic Plan*. The proposed NPCC 2021 Corporate Goals are an expansion of the many objectives outlined in the Board and FERC approved *NPCC 2021 Business Plan and Budget*. For each NPCC Goal, Threshold and Target performance levels are identified. Attainment of a previous performance level is a pre-requisite for credit of attainment at a higher performance level. In addition, each aspect of a goal has been classified as either Qualitative or Quantitative, and a third-party oversight reviewer has been identified to support objectivity and enhance auditability.

A summary of the proposed NPCC 2021 Corporate Goals appears on the next page, with the full set of supporting milestones for the NPCC 2021 Corporate Goals included on the subsequent pages.



NPCC 2021 CORPORATE RELIABILITY GOALS

<i>Goal</i>	<i>Reliability Goal Objectives</i>	<i>Qualitative and Quantitative</i>	<i>Oversight Reviewer</i>
IA - (25%)	Goal Objective: Enhance System Resilience <i>Assess operational resilience, inherent risks, and critical infrastructure interdependencies within Northeastern North America.</i>	<i>X</i>	<i>Reliability Coordinating and Compliance Committees</i>
IB - (25%)	Goal Objective: Assure Energy Sufficiency <i>Enhance assessment of energy sufficiency utilizing advanced probabilistic approaches, improved modeling, and evaluation of non-peak periods.</i>	<i>X</i>	<i>Reliability Coordinating and Regional Standards Committees</i>
II – (25%)	Goal Objective: Reliably Integrate Resources Supporting De-Carbonization Objectives, Including DER) <i>Support reliable integration of resources associated with carbon emissions objectives and coordinate review/revision of NPCC documents to identify potential barriers to de-carbonization.</i>	<i>X</i>	<i>Regional Standards and Reliability Coordinating Committees</i>
III - (25%)	Goal Objective: Address Cyber and Physical Security Threats <i>Support mitigation of cyber and physical security threats within Northeastern North America.</i>	<i>X</i>	<i>Reliability Coordinating and Compliance Committees</i>



NPCC 2021 CORPORATE RELIABILITY GOALS

IA.	Enhance System Resilience	Weighting: 25% of Total	
	Assess operational resilience, inherent risks, and critical infrastructure interdependencies within Northeastern North America.	Threshold	Target
IA-1. (10%)	Utilize the North American Transmission Forum's (NATF) Transmission Resilience Maturity Model (TRMM) within NPCC to enhance the resilience of the Northeastern North America transmission system.	Recruit three (3) NPCC Transmission Owners to share an overview of their TRMM to evaluate its applicability for assessing transmission resilience – by 9/21.	Develop recommendations for NPCC Region-wide use of the TRMM to further NPCC's resilience objectives for endorsement by RCC – by 12/21.
IA-2. (10%)	Enhance the NPCC Compliance Oversight Plan (COP) process for entities outside of the schedule of audits in order to early identify key risk categories.	Enhance COP methodology to include additional performance considerations and criteria that assist in identifying priority standards. Obtain CC acceptance of performance consideration criteria – by 5/21. Present at the NPCC Spring 2021 webinar.	Perform enhanced COP process on ten (10) entities not on 2021 audit schedule – by 11/21. Present results to CC – by 12/21 Present status at NPC Fall 2021 webinar.



NPCC 2021 CORPORATE RELIABILITY GOALS

IA-3. (5%)	Assess critical telecommunication infrastructure interdependency risks, and identify mitigation opportunities to enhance system resilience.	Identify telecommunication system interdependency risks associated with restoration activities. Status to the RCC – by 5/21.	Develop recommendation(s) and identify best currently available practice(s) to mitigate telecommunication interdependency risks for RCC endorsement – by 12/21.

I-B.	Assure Energy Sufficiency	Weighting: 25% of total	
	Enhance assessment of energy sufficiency utilizing advanced probabilistic approaches, improved modeling, and evaluation of non-peak periods.	Threshold	Target
IB-1. (10%)	Expand NPCC's assessment of Loss of Load Hours (LOLH - hours/year) and Expected Unserved Energy (EUE – MWh/year) impacts in the evaluation of the NPCC Balancing Authority Area (BAA) resource adequacy plans to address societal decarbonization objectives.	Develop an advanced probabilistic representation of the NPCC system suitable for the resource adequacy assessment of NPCC's future societal decarbonization objectives. Present for RCC endorsement – by 5/21.	Utilizing LOLH and EUE to assess BAA resource adequacy impacts associated with societal decarbonization objectives within NPCC. Present report to the RCC for endorsement – by 12/21.



NPCC 2021 CORPORATE RELIABILITY GOALS

IB-2. (10%)	Enhance modeling for aggregated DER, Energy Limited Resources (ELR) (such as energy storage) and Variable Energy Resources (VER) in NPCC probabilistic resource adequacy assessments.	Identify best currently available aggregated DER, ELR and VER advanced modeling practice(s) to the RCC – by 5/21.	Demonstrate the enhanced reliability impact accuracy of advanced aggregated DER, ELR and VER modeling in NPCC probabilistic resource adequacy assessments. Provide recommendations for RCC endorsement – by 12/21.
IB-3. (5%)	Assess the future reliability risk to the BPS of a significant gas contingency during periods of increased reliance on natural gas, including electrical non-peak/shoulder months periods.	Develop a gas-electric model suitable for the analysis of NPCC winter and off-peak periods. Present model and analytical approach to the RCC for endorsement – by 5/21.	Report the results of the NPCC gas-electric risk assessment to the RCC for endorsement – by 12/21.

NPCC 2021 CORPORATE RELIABILITY GOALS

II.	Reliably Integrate Resources Supporting De-Carbonization Objectives, Including Distributed Energy Resources (DER)	Weighting: 25% of Total	
	Support reliable integration of resources associated with carbon emissions objectives and coordinate review/revision of NPCC documents to identify potential barriers to de-carbonization.	Threshold	Target
II-1. (20%)	Expand the DER Forum topics to include reliable integration of VER on the BPS (e.g. Offshore Wind). Review NPCC documents for any potential revisions in the context of a de-carbonized future. Identify any emerging reliability risk areas for VER and DER deployment not already actively being addressed by the ERO Enterprise.	Expand the reliability scope of activities of the NPCC DER Forum to include VER and conduct three DER Forums. Develop a draft whitepaper for identifying and prioritizing which Directories should be revised to accommodate de-carbonization objectives and increased amounts of DER and VER for RSC and RCC endorsement – by 10/21.	Draft Version 3 of the NPCC DER Guidance document to include emerging technological advancements, advanced inverter application and functions, and emerging reliability concerns from increased deployment of DER and post for a 45-day industry comment – by 12/21.
II-2. (5%)	Enhance outreach to states, provinces, planning authorities and other stakeholders to establish a higher degree of coordination and transparency during the energy transition brought forward by societal de-carbonization objectives.	Conduct three briefings with state and provincial regulators on NERC and NPCC reliability assessments and evolving DER and VER societal objectives– by 12/21.	Develop long-term strategic reliability recommendations incorporating input from state and provincial regulators relating to their de-carbonization goals for RSC and RCC endorsement by 12/21.



NPCC 2021 CORPORATE RELIABILITY GOALS

III.	Address Cyber and Physical Security Threats	Weighting; 25% of Total	
	Support mitigation of cyber and physical security threats within Northeastern North America.	Threshold	Target
III-1. (5%)	Advance best currently available approaches to mitigating entities' security risks/threats, including strengthening interactions between critical infrastructure sectors	Conduct three (3) joint physical and cyber security collaboration sessions with Gas Sector representatives. Present coordination recommendations to the RCC for endorsement – by 9/21.	Perform two (2) Design Basis Threat training exercises for NPCC entities to enhance their security posture – by 11/21. Report non-proprietary findings and recommendations for RCC endorsement – by 12/21.
III-2. (10%)	Transition NPCC's 210 registered entities from the current compliance program (CDAA) through the three (3) currently scheduled releases of the new Align and Secure Evidence Locker (SEL) tools to ensure ERO Enterprise-wide compatibility and that the enhanced security benefits for the handling of entity data/evidence are realized as per the NERC project deadlines.	Develop prioritized 2021 strategy for entity training to CC for endorsement - by 3/21. Complete training for registered entities on Align/SEL Release 1 - by 4/21. Present user survey on NPCC R1 training to CC – by 5/21.	Complete training for registered entities on Align/SEL Release 2 and Release 3 - by 6/21 and 12/21, respectively. Present user survey on overall NPCC training to CC for endorsement – by 12/21.



NPCC 2021 CORPORATE RELIABILITY GOALS

III-3. (10%)	Expand interaction with the E-ISAC to identify and raise registered entity awareness of cybersecurity threats to the Northeastern North America.	Issue TFIST endorsed Quarterly Security Awareness Bulletins on cyber threats (e.g., supply chain attacks, phishing, credential theft). Develop a cyber threat awareness presentation for TFIST and RCC comment and endorsement – by 6/21. Develop best currently available practice(s) that entities can use to reduce the risk of cyber-attacks.	Present best currently available practice(s) to TFIST for comment and the RCC for endorsement - by 9/21. Present endorsed best currently available practice(s) via Webinar to industry - by 12/21

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	08/19/15
SAR posted for comment	08/20/15 – 09/21/15
Draft Reliability Standard posted for Informal Comment Period	07/14/16 – 08/12/16
45-day formal comment period with ballot	09/29/17 – 11/14/17
45-day formal comment period with ballot	08/24/19 – 10/17/18
45-day formal comment period with additional ballot	06/19/20 – 08/26/20

Anticipated Actions	Date
45-day formal comment period with additional ballot	October 2020
10-day final ballot	December 2020
NERC Board adoption	February 2021

A. Introduction

1. **Title:** Establish and Communicate System Operating Limits
2. **Number:** FAC-014-3
3. **Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies and that Planning Assessment performance criteria is coordinated with these methodologies.
4. **Applicability:**
 - 4.1. **Functional Entities:**
 - 4.1.1. Planning Coordinator
 - 4.1.2. Reliability Coordinator
 - 4.1.3. Transmission Operator
 - 4.1.4. Transmission Planner
5. **Effective Date:** See Implementation Plan for [Project 2015-09](#).

B. Requirements and Measures

- R1. Each Reliability Coordinator shall establish Interconnection Reliability Operating Limits (IROLs) for its Reliability Coordinator Area in accordance with its System Operating Limit methodology (SOL methodology). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*
- M1. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation that demonstrates the Reliability Coordinator established IROLs in accordance with its SOL methodology.
- R2. Each Transmission Operator shall establish System Operating Limits (SOLs) for its portion of the Reliability Coordinator Area in accordance with its Reliability Coordinator's SOL methodology. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- M2. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation that demonstrates the Transmission Operator established SOLs in accordance with its Reliability Coordinator's SOL methodology.
- R3. Each Transmission Operator shall provide its SOLs to its Reliability Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-day Operations, Real-Time Operations]*

- M3.** Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation that demonstrates the Transmission Operator provided its SOLs ~~in accordance with its Reliability Coordinator's SOL methodology.~~
- R4.** Each Reliability Coordinator shall establish stability limits when ~~the limit~~ an instability impacts adjacent Reliability Coordinator Areas or more than one Transmission Operator in its Reliability Coordinator Area in accordance with its SOL methodology. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*
- M4.** Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation that demonstrates the Reliability Coordinator established stability limits in accordance with Requirement R4.
- R5.** Each Reliability Coordinator shall provide: *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-day Operations, Real-Time Operations]*
- 5.1** Each Planning Coordinator and each Transmission Planner within its Reliability Coordinator Area, the SOLs for its Reliability Coordinator Area (including the subset of SOLs that are IROLs) at least once every twelve calendar months.
- 5.2** Each impacted Planning Coordinator and each impacted Transmission Planner within its Reliability Coordinator Area, the following information for each established stability limit and each established IROL at least once every twelve calendar months:
- 5.2.1** The value of the stability limit or IROL;
- 5.2.2** Identification of the Facilities that are critical to the derivation of the stability limit or the IROL;
- 5.2.3** The associated IROL T_v for any IROL;
- 5.2.4** The associated critical Contingency(ies);
- 5.2.5** A description of system conditions associated with the stability limit or IROL; and
- 5.2.6** The type of limitation represented by the stability limit or IROL (*e.g.*, voltage collapse, angular stability).
- 5.3** Each impacted Transmission Operator within its Reliability Coordinator Area, the value of the stability limits established pursuant to Requirement R4 and each IROL established pursuant to Requirement R1, in an agreed upon time frame necessary for inclusion in the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
- 5.4** Each impacted Transmission Operator within its Reliability Coordinator Area, the information identified in Requirement R5 Parts 5.2.2 – 5.2.6 for each established stability limit ~~or~~ and each established IROL, and any updates to that information within an agreed upon time frame necessary for inclusion in the Transmission Operator's Operational Planning Analyses.

5.5 Each requesting Transmission Operator within its Reliability Coordinator Area, requested SOL information for its Reliability Coordinator Area, on a mutually agreed upon schedule.

5.55.6 Each impacted Generator Owner or Transmission Owner, within its Reliability Coordinator Area, with a list of their Facilities that have been identified as critical to the derivation of an IROL and its associated critical contingencies.

M5. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation, posting to a secure website, or other electronic means, that demonstrates the Reliability Coordinator provided the information in accordance with Requirement R5.

~~R7~~R6. Each Planning Coordinator and each Transmission Planner shall implement a documented process to use Facility Ratings, System steady-state voltage limits and stability criteria in its Planning Assessment of Near Term Transmission Planning Horizon that are equally limiting or more limiting than the criteria for Facility Ratings, System Voltage Limits and stability described in its respective Reliability Coordinator's SOL methodology. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- The Planning Coordinator may use less limiting Facility Ratings, System steady-state voltage limits and stability criteria if it provides a technical rationale to each affected Transmission Planner, Transmission Operator and Reliability Coordinator.
- The Transmission Planner may use less limiting Facility Ratings, System steady-state voltage limits and stability criteria if it provides a technical rationale to each affected Planning Coordinator, Transmission Operator and Reliability Coordinator.

M6. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator and Transmission Planner implemented its documented process in accordance with Requirement R6.

~~R8~~R7. Each Planning Coordinator and each Transmission Planner shall annually communicate the following information for Corrective Action Plans developed to address any instability identified in its Planning Assessment of the Near-Term Transmission Planning Horizon to each impacted Transmission Operator and Reliability Coordinator. This communication shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- 7.1** The Corrective Action Plan developed to mitigate the identified instability, including any automatic control or operator-assisted actions (such as Remedial Action Schemes, under voltage load shedding, or any Operating Procedures);
- 7.2** The type of instability addressed by the Corrective Action Plan (e.g. steady-state and/or transient voltage instability, angular instability including generating unit loss of synchronism and/or unacceptable damping);
- 7.3** The associated stability criteria violation requiring the Corrective Action Plan (e.g. violation of transient voltage response criteria or damping rate criteria);

- 7.4 The planning event Contingency(ies) associated with the identified instability requiring the Corrective Action Plan;
- 7.5 The System conditions and Facilities associated with the identified instability requiring the Corrective Action Plan.
- M7. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator and Transmission Planner communicated the information in accordance with Requirement R7.

~~R10, R8.~~ Each Planning Coordinator and each Transmission Planner shall annually communicate ~~any instability, Cascading or uncontrolled separation that adversely impact the reliability of the Bulk Electric System identified in its Planning Assessment of the Near-Term Transmission Planning Horizon~~ to each impacted Transmission Owner and Generation Owner a list of their Facilities that comprise the planning event Contingency(ies) that would cause. ~~This communication shall include those Facilities that comprise the Contingency(ies) (planning events only) and any Facilities critical to the~~ instability, Cascading or uncontrolled separation that adversely impacts the reliability of the BES as identified in its Planning Assessment of the Near-Term Transmission Planning Horizon identified. [Violation Risk Factor: Medium] [Time Horizon: Long- term Planning]

~~M9, M8.~~ Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator and Transmission Planner communicated the information in accordance with Requirement R8.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

“Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) 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 applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Reliability Coordinator, Transmission Operator, Transmission Planner, Planning Coordinator shall keep data or evidence of Requirements R1 through R8 for the current year plus the previous 12 calendar months.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Reliability Coordinator failed to establish Interconnection Reliability Operating Limits (IROLs) for its Reliability Coordinator Area in accordance with its System Operating Limit Methodology (“SOL methodology”) as established in FAC-011-4.
R2.	N/A	N/A	N/A	The Transmission Operator failed to establish SOLs for its portion of the Reliability Coordinator Area in accordance with its Reliability Coordinator’s SOL methodology.
R3.	N/A	N/A	The Transmission Operator provided its SOLs to its Reliability Coordinator, but failed to provide its SOLs at the periodicity at which the Reliability Coordinator needs	The Transmission Operator failed to provide its SOLs to its Reliability Coordinator.

			such information to perform its reliability functions.	
R4.	N/A	N/A	N/A	The Reliability Coordinator failed to establish stability limits to be used in operations when the limit impacts an adjacent Reliability Coordinator or more than one Transmission Operator in its Reliability Coordinator Area in accordance with its SOL methodology.
R5.	The Reliability Coordinator failed to provide one of the items listed in Requirement R5, Parts 5.1 through 5.56.	The Reliability Coordinator failed to provide two of the items listed in Requirement R5, Parts 5.1 through 5.56.	The Reliability Coordinator failed to provide three of the items listed in Requirement R5, Parts 5.1 through 5.56.	The Reliability Coordinator failed to provide four or more of the items listed in Requirement R5, Parts 5.1 through 5.56.
R6.	N/A	N/A	The Planning Coordinator or a Transmission Planner used less limiting Facility Ratings, System steady state voltage limits or stability criteria than the criteria for Facility Ratings, System Voltage Limits or stability described in its respective Reliability Coordinator's SOL methodology, but failed to	The Planning Coordinator or a Transmission Planner failed to implement a process to ensure that Facility Ratings, System steady state voltage limits or stability criteria used in Planning Assessment are equally limiting or more limiting than the criteria for Facility Ratings, System Voltage Limits or stability

			provide a technical rationale for allowing the use of less limiting Facility Ratings, System Voltage Limits or stability criteria	described in its respective Reliability Coordinator's SOL methodology.
R7.	The Planning Coordinator or a Transmission Planner communicated the identified instability to each impacted Reliability Coordinator and Transmission Operator, but the communication did not contain one of the elements listed in Requirement R7, Parts 7.1 through 7.5.	The Planning Coordinator or a Transmission Planner communicated the identified instability to each impacted Reliability Coordinator and Transmission Operator, but the communication did not contain two of the elements listed in Requirement R7, Parts 7.1 through 7.5.	The Planning Coordinator or a Transmission Planner communicated the identified instability to each impacted Reliability Coordinator and Transmission Operator, but the communication did not contain three elements listed in Requirement R7, Parts 7.1 through 7.5.	The Planning Coordinator or a Transmission Planner communicated the identified instability to each impacted Reliability Coordinator and Transmission Operator, but the communication did not contain four or more of the elements listed in Requirement R7, Parts 7.1 through 7.5. OR The Planning Coordinator or a Transmission Planner failed to communicate any identified instability, to each impacted Reliability Coordinator and Transmission Operator.
R8.			The Planning Coordinator or a Transmission Planner provided the instability, Cascading or uncontrolled separation information listed	The Planning Coordinator or a Transmission Planner failed to provide the instability, Cascading or uncontrolled separation information listed

			in Requirement R8 to the applicable Transmission Owner, and Generation Owner, but failed to provide them annually.	in Requirement R8 to the applicable Transmission Owner, and Generation Owner.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board	New
2		Changed the effective date to January 1, 2009 Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	June 24, 2008	Adopted by Board: FERC Order	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	April 29, 2015 – July 23, 2015	Incorrectly included TOP as the applicable function for Requirement R5. 7/23/15: Corrected to designate R5 as: RC, PA and TP.	Revised
<u>3</u>		<u>Project 2015-09 Adopt revised standard.</u>	<u>Revised</u>

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization
2. **Number:** CIP-002-~~76~~
3. **Purpose:** To identify and categorize BES Cyber Systems (~~BES Cyber Systems~~BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the BES. Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider that owns** 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 Remedial Action Scheme (RAS) where the ~~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. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. 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 ~~Remedial Action Scheme~~RAS where the ~~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-002-76:

4.2.3.1. Cyber Assets-systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets-systems associated with communication networks and data communication links between discrete Electronic Security Perimeters logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.2.4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.3.4.2.3.4. 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.

4.2.3.4.4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Date: See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-002-6.~~

6. Background: This standard provides “bright line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements 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 and the criteria in Attachment 1 of CIP-002 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. 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.

BES Cyber Systems

The CIP Cyber Security Standards use the “BES Cyber System” term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware

protection to a grouping rather than individual Cyber Assets and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term “BES Cyber System” is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity’s responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement R1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 — Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

- ~~• **Electronic Access Control or Monitoring Systems (“EACMS”)** — Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
- ~~• **Physical Access Control Systems (“PACS”)** — Examples include: authentication servers, card systems, and badge control systems.~~
- ~~• **Protected Cyber Assets (“PCA”)** — Examples include, to the extent they are within the ESP: file servers, FTP servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*
- i. Control Centers and backup Control Centers;
 - ii. Transmission stations and substations;
 - iii. Generation resources;
 - iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
 - v. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System; and
 - vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
- 1.1.** Identify each of the high impact ~~BES Cyber System~~BCS according to Attachment 1, Section 1, if any, at each asset;
- 1.2.** Identify each of the medium impact ~~BES Cyber System~~BCS according to Attachment 1, Section 2, if any, at each asset; and
- 1.3.** Identify each asset that contains a low impact ~~BES Cyber System~~BCS or SCI that hosts any portion of a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~BCS or SCI that hosts any portion of a low impact BCS is not required).
- 1.4.** Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).
- 1.5.** Identify associated SCI that hosts any portion of the medium impact ~~BES Cyber System~~BCS identified in Part 1.2 above or their associated EACMS, PACS or PCAs.
- M1.** Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, ~~and Parts 1.1, and 1.2, 1.4 and 1.5.~~
- R2.** Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- 2.1.** Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and
 - 2.2.** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

- M2.** Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) 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 Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.4. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Operations Planning	High	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~SystemsBCS, and associated SCI~~, five percent or fewer of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, five or fewer identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and ~~BES Cyber SystemsBCS and associated SCI~~, more than five but less than or equal to 10 identified ~~BES Cyber~~	For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and ~~BES Cyber AssetsBCS and associated SCI~~, more than 10 but less than or equal to 15 identified ~~BES Cyber~~	~~SystemsBCS and associated SCI~~, more than 15 percent of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than 15 identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber SystemsBCS, and associated SCI~~, five percent or fewer high or medium ~~BES Cyber SystemsBCS or associated SCI~~, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber SystemsBCS, or associated SCI~~, five or fewer high or medium ~~BES Cyber SystemsBCS or associated SCI~~, have not been identified.	~~SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber SystemsBCS or associated SCI~~ have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	~~Assets-BCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber SystemsBCS or associated SCI~~ have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than 15 percent of high or medium impact ~~BES Cyber SystemsBCS or associated SCI~~ have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than 15 high or medium impact ~~BES Cyber SystemsBCS or associated SCI~~ have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Cyber Systems~~ BCS and associated SCI, more than five but less than or equal to 10 high or medium ~~BES Cyber Systems~~ BCS or associated SCI have not been identified.	~~Cyber Systems~~ BCS and associated SCI, more than 10 but less than or equal to 15 high or medium ~~BES Cyber Systems~~ BCS or associated SCI have not been identified.	
R2.	Operations Planning	Lower	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 15 calendar months but less than or equal to 16 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity did not complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 16 calendar months but less than or equal to 17 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 17 calendar months but less than or equal to 18 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 18 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity failed to complete its approval of the identifications required by <u>Requirement R1</u> by the CIP Senior Manager or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002- ~~76~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>Requirement</u> R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)	<u>Requirement</u> R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)	<u>Requirement</u> R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)	delegate according to Requirement R2 within 18 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan for CIP-002-~~76~~.”
- ~~See Appendix 1. The Interpretation in Appendix 1 was developed under a prior version of the Reliability Standard, CIP-002-5.1, and is being carried forward to subsequent versions.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating

Each ~~BES Cyber System~~BCS used by and located at any of the following:

- 1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
- 1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
- 1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
- 1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating

Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those each discrete~~ shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
- 2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are those shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.
- 2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

- 2.4.** Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
- 2.5.** Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

- 2.6.** Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 2.7.** Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 2.8.** Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.
- 2.9.** Each ~~Remedial Action Scheme (RAS)~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.
- 2.10.** Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

- 2.11.** Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.
- 2.12.** Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

- 2.13.** Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

- 3.1.** Control Centers and backup Control Centers.
- 3.2.** Transmission stations and substations.
- 3.3.** Generation resources.
- 3.4.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

- 3.5. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System.
- 3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

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 qualified 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. This section is especially significant in CIP-002-6 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-6. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-6

CIP-002-6 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “...that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-6. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions

- ~~Balancing Load and Generation~~
- ~~Controlling Frequency (Real Power)~~
- ~~Controlling Voltage (Reactive Power)~~
- ~~Managing Constraints~~
- ~~Monitoring & Control~~
- ~~Restoration of BES~~
- ~~Situational Awareness~~
- ~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

Entity Registration	BC	BA	TDP	TD	DP	GDP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
 - ~~Providing actual reserve generation when called upon (GO, GOP)~~
 - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
 - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
 - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
 - ~~Zone protection for breaker failure (DP, TO, TOP)~~
 - ~~Breaker protection (DP, TO, TOP)~~
 - ~~Current, frequency, speed, phase (TO, TOP, GO, GOP)~~
- ~~Remedial Action Schemes~~
 - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
 - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
 - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- ~~Calculation of Area Control Error (ACE)~~
 - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
 - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
 - ~~Ability to identify load change need (BA)~~
 - ~~Ability to implement load changes (TOP, DP)~~
- ~~Manually Initiated Load shedding~~
 - ~~Ability to identify load change need (BA)~~
 - ~~Ability to implement load changes (TOP, DP)~~
- ~~Non spinning reserve (contingency reserve)~~

- Know generation status, capability, ramp rate, start time (GO, BA)
- Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
 - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
 - Software to calculate unit adjustments (BA)
 - Transmit adjustments to individual units (GOP)
 - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
 - Frequency source, schedule (BA)
 - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
 - Sensors, stator control system, feedback (GO)
- Capacitive resources
 - Status, control (manual or auto), feedback (TOP, TO, DP)
- Inductive resources (transformer tap changer, or inductors)
 - Status, control (manual or auto), feedback (TOP, TO, DP)
- Static VAR Compensators (SVC)
 - Status, computations, control (manual or auto), feedback (TOP, TO, DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)

- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

Monitoring and Control

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches
 - ~~SCADA (TOP, GOP)~~
 - ~~Substation automation (TOP)~~~~

Restoration of BES

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path
 - ~~Through black start units (TOP, GOP)~~
 - ~~Through tie lines (TOP, GOP)~~~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

Situational Awareness

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC, BA)~~
- ~~Change management (TOP, GOP, RC, BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

Inter-Entity Coordination

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and~~

operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- ~~Scheduled interchange (BA, TOP, GOP, RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

When the drafting team uses the term “Facilities,” there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as, “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-6, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may

~~be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~

~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~

~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

High Impact Rating

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

Medium Impact Rating

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high impact.~~

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is “to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance.” In particular, it requires that “as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency.” The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a “long term” reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as “Reliability Must Run,” and this designation is distinct from those generation Facilities designated as “must run” for market stabilization purposes. Because the use of the term “must run” creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units

~~designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL 003, then BES Cyber Systems for that unit are categorized as medium impact.~~

~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~● Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.~~

~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~● Criterion 2.9 categorizes BES Cyber Systems for Remedial Action Schemes as medium impact. Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~
- ~~● Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~
- ~~● Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500-MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

Transmission

~~The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical~~

~~borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.~~

- ~~● Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~
- ~~● Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the “Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface.” This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~● Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~
 - ~~■ Excluded radial facilities that would only provide support for single generation facilities.~~
 - ~~■ Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

Additionally, in Attachment 1 of NERC's "Integrated Risk Assessment Approach—Refinement to Severity Risk Index" document, the report used an average MVA line loading based on kV rating:

- ~~230 kV → 700 MVA~~
- ~~345 kV → 1,300 MVA~~
- ~~500 kV → 2,000 MVA~~
- ~~765 kV → 3,000 MVA~~

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~
- ~~Multiple point (or multiple tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

- ~~1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~

- ~~2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4.: there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~• Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC 014 2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.~~
- ~~• Criterion 2.7 is sourced from the NUC 001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC 001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~
- ~~• Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide-area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~
- ~~• Criterion 2.9 designates as medium impact those BES Cyber Systems for those Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~
- ~~• Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted~~

~~that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. 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.~~

~~In ERCOT, the Load acting as a Resource (“Laar”) Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~• Criterion 2.12 categorizes medium impact BES Cyber Systems associated with Control Centers and backup Control Centers, including associated data centers, that monitor and control BES Transmission Lines with an aggregate weighted value of 6000 or higher, and that have not already been included in Part 1. The drafting team included additional qualifications in this criterion that would ensure the required level of impact to the BES is defined and a risk threshold associated to establish a floor for applicable medium impact BES Cyber Systems.~~

~~The total aggregated weighted value is used to account for the impact to the BES. The 6000 aggregate weighted value threshold defined in criterion 2.12 provides a sufficient differentiation for medium and low impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission Lines. SDT analysis of Transmission Control Centers validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.~~

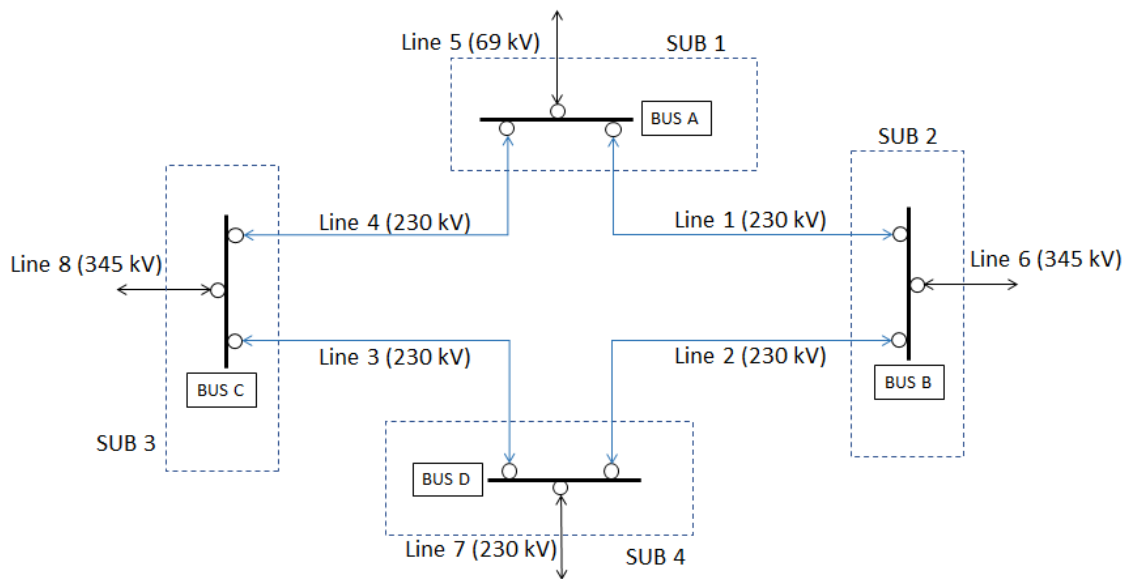
~~In the terms of applicable BES Transmission Lines, the following should be considered:~~

- ~~▪ All BES Transmission Lines that are energized at voltages between 100 kV and 499 kV and are monitored and controlled by a Control Center, including associated data center(s).~~

- All BES Transmission Lines, including those that connect to neighboring entities, that are monitored and controlled by the Responsible Entity's Control Center, including associated data center(s).
- Multiple point (or multiple tap) lines are considered to contribute a single weight value per line. For example, a single 230 kV multiple point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. For example, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.12 Examples:

In example 1 below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.



Example 1

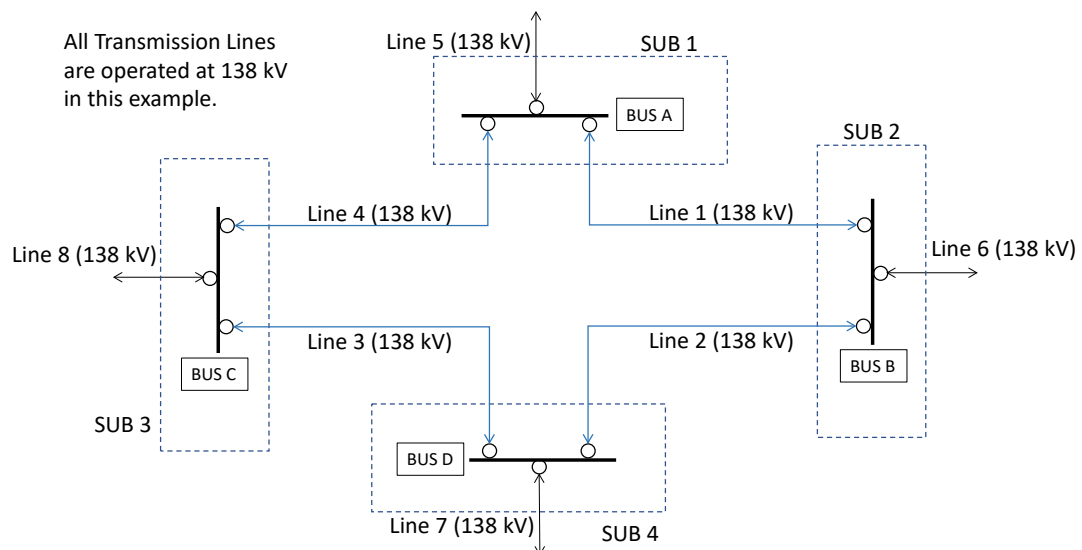
The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. In accordance with Criterion 2.12, the BES Cyber System(s) associated with the Control Center should be categorized as medium impact BES Cyber System(s).

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~Line 5~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~None~~	~~0~~
~~200 kV to 299 kV~~	~~700~~	~~Line 1, Line 2, Line 3, Line 4, Line 7~~	~~3500~~
~~300 kV to 499 kV~~	~~1300~~	~~Line 6, Line 8~~	~~2600~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

Calculation

$$700+700+700+700+700+1300+1300 = 6100$$

In the additional example below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.



Example 2

The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 2000, which is below the minimum threshold for a medium impact rating required in Criterion 2.12. The BES Cyber System(s) associated with the Control Center in this example should be categorized as a low impact BES Cyber System(s) pursuant to Criterion 3.1.

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
less than 100 kV (not applicable)	(not applicable)	None	N/A
100 kV to 199 kV	250	Line 1, Line 2, Line 3, Line 4, Line 5, Line 6, Line 7, Line 8	2000
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	None	0
500 kV and above	0	None	0

Calculation

$$250+250+250+250+250+250+250+250= 2000$$

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating

No additional evaluation is necessary for BES Cyber Systems that have already been identified as high or medium impact. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact. Note that low impact BES Cyber Systems do not require discrete identification, only identification of the asset containing the low impact BES Cyber System(s).

Restoration Facilities

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection~~

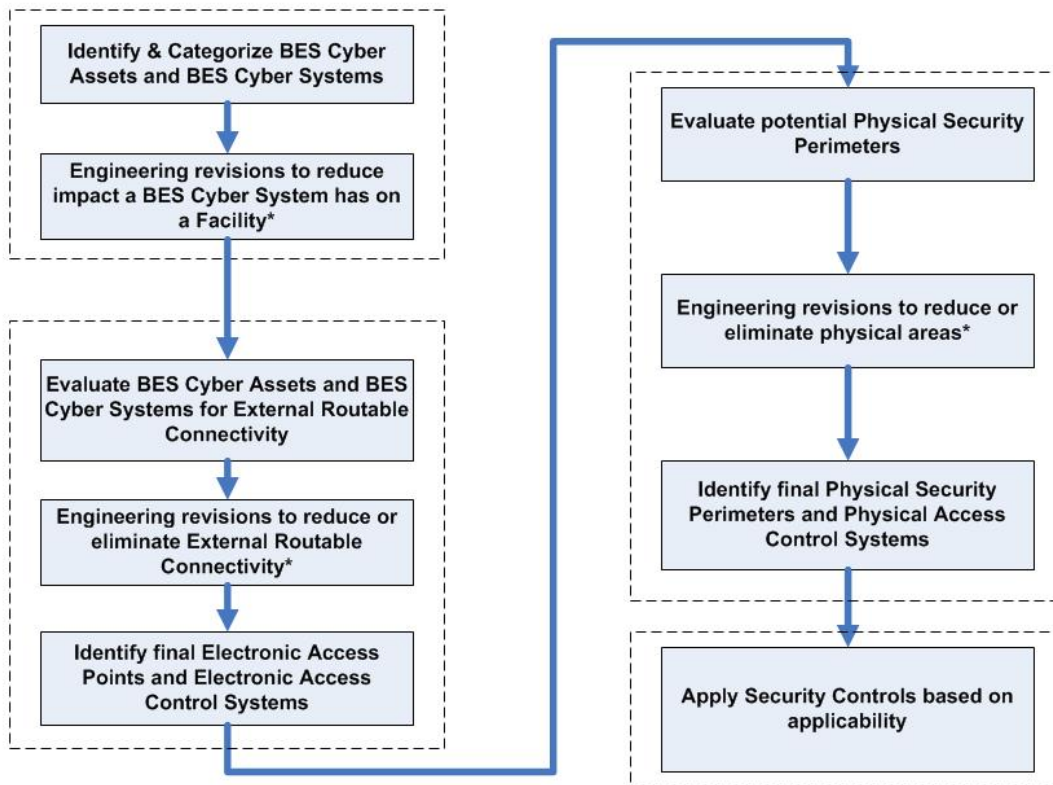
~~point of the generation unit(s) to be started, as identified in the Transmission Operator’s restoration plan, default to the category of low impact; however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator’s Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~

Overview (Generation Facility)



* - Engineering revisions will need to be reviewed for cost justification, operational safety requirements, support requirements, and technical limitations.

Rationale

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

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of “bright line” criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real time operation of the BES. The CIP Senior Manager’s approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

1

Requirement Number and Text of Requirement

CIP-002 5.1, Requirement R1

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

- i. Control Centers and backup Control Centers;
- ii. Transmission stations and substations;
- iii. Generation resources;
- iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

- ~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~

~~Attachment 1, Criterion 2.1~~

~~2. Medium Impact Rating (M)~~

~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~

- ~~2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

Questions

~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase “shared BES Cyber Systems.”~~

~~The Interpretation Drafting Team identified the following questions in the RFI:~~

- ~~1. Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~
- ~~2. Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~
- ~~3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

Responses

~~**Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?**~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify each of~~

~~the medium impact BES Cyber Systems according to Attachment 1, Section 2...~~ Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states ~~“Each BES Cyber System...associated with any of the following [criteria].”~~ (emphasis added)

~~Additionally, the Background section of CIP-002-5.1 states that “[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System.” The Background section also provides:~~

~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Question 2: Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~

~~The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.” For criterion 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.~~

~~Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-~~98~~
3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) 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 Remedial Action Scheme (RAS) where the 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. **Reliability Coordinator**
 - 4.1.6. **Transmission Operator**

4.1.7. 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 Section 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 RAS where the 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-003-98:

4.2.3.1. Cyber Assets-systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets-systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters (ESPs)~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.2.4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.4.2.3.4.~~ 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.

~~4.2.3.4.4.2.3.5.~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project CIP-003-8~~

~~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 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

- 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~~BCS and associated SCI, 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~~BCS (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~~BCS (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~~BCS and associated SCI, if any:
 - 1.2.1.** Cyber security awareness;
 - 1.2.2.** Physical security controls;
 - 1.2.3.** Electronic access controls;
 - 1.2.4.** Cyber Security Incident response;
 - 1.2.5.** Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and
 - 1.2.6.** Declaring and responding to CIP Exceptional Circumstances.
- 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.
- R2.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact ~~BES Cyber Systems~~BCS and their associated SCI 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~~BCS or their associated SCI ~~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.
- 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.
- 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 Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.3. Compliance Monitoring and Assessment Processes:~~

- ~~• Compliance Audits~~
- ~~• Self-Certifications~~
- ~~• Spot-Checking~~
- ~~• Compliance Investigations~~
- ~~• Self-Reporting~~
- ~~• Complaints~~

~~1.4. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			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~~ <u>BCS and associated SCI</u> but did not address one of the nine topics required by <u>Requirement R1. (Requirement R1 Part 1.1)</u> 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~~ <u>BCS</u>	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ <u>BCS and associated SCI</u> but did not address two of the nine topics required by <u>Requirement R1. (Requirement R1 Part R1.1)</u> 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~~ <u>BCS</u>	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ <u>BCS and associated SCI</u> but did not address three of the nine topics required by <u>Requirement R1. (Requirement R1 Part R1.1)</u> 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~~ <u>BCS and associated SCI</u> as required by <u>Requirement</u>	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ <u>BCS and associated SCI</u> but did not address four or more of the nine topics required by <u>Requirement R1. (Requirement R1 Part R1.1)</u> OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ <u>BCS and associated SCI</u> as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>and associated SCI</u> as required by <u>Requirement R1</u> within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (<u>Requirement R1 Part 1.1</u>) 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~~ <u>BCS and associated SCI</u> as required by <u>Requirement R1</u> by the CIP Senior	<u>and associated SCI</u> as required by <u>Requirement R1</u> within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (<u>Requirement R1 Part 1.1</u>) 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 <u>BCS and associated SCI</u> as required by <u>Requirement R1</u> by the CIP Senior	R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (<u>Requirement R1 Part 1.1</u>) 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~~ <u>BCS and associated SCI</u> as required by <u>Requirement R1</u> 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. (<u>Requirement R1</u>)	required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by <u>Requirement R1</u> within 18 calendar months of the previous review. (<u>Requirement R1</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but did not address one of the six topics required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.2</u>)	Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but did not address two of the six topics required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.2</u>)	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~, but did not address three of the six topics required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.2</u>) 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 BCS and associated SCI~~ as required by <u>Requirement R1</u> within 17 calendar	medium impact ~~BES Cyber Systems BCS and associated SCI~~ as required by <u>Requirement R1</u> by the CIP Senior Manager within 18 calendar months of the previous approval. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but did not address four or more of the six topics required by <u>Requirement R1</u>.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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~~ <u>Cyber Systems BCS and associated SCI</u> as 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. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its	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~~ <u>Cyber Systems BCS and associated SCI</u> as 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. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its	months but did complete this review in less than or equal to 18 calendar months of the previous review. (<u>Requirement R1 Part 1.2</u>) 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 BCS and associated SCI~~ 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.	(<u>Requirement R1 Part 1.2</u>) 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 BCS and associated SCI~~ as required by Requirement R1. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES-Cyber Systems BCS~~ and associated SCI as required by Requirement 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 the previous approval. (<u>Requirement R1 Part R1.2</u>)	approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES-Cyber Systems BCS~~ and associated SCI as required by Requirement 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 the previous approval. (<u>Requirement R1 Part R1.2</u>)	(<u>Requirement R1 Part R1.2</u>)	in CIP-002 containing low impact ~~BES-Cyber Systems BCS~~ and associated SCI as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (<u>Requirement R1 Part R1.2</u>)
R2	Operations Planning	Lower	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	The Responsible Entity documented the physical access controls for its assets containing low impact ~~BES-Cyber~~	The Responsible Entity failed to document and implement one or more cyber security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (<u>Requirement R2</u>) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (<u>Requirement R2</u>) OR The Responsible Entity documented	impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (<u>Requirement R2</u>) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to document physical security controls according to Requirement R2, Attachment 1,	~~Systems BCS and associated SCI~~ but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (<u>Requirement R2</u>) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (<u>Requirement R2</u>) OR	plan(s) for its assets containing low impact ~~BES Cyber Systems BCS and associated SCI~~ according to Requirement R2, Attachment 1. (<u>Requirement R2</u>)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u> but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u>	Section 2. (<u>Requirement</u> R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u> but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (<u>Requirement</u> R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all	The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u> but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to manage its <u>TCA</u> according to Requirement R2, Attachment 1, Section 5.1. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u>, but failed to	Dial-up Connectivity that provides access to low impact ~~BES~~ <u>Cyber System(s)</u> <u>BCS</u>, per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (<u>Requirement</u> R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES~~ <u>Cyber Systems</u> <u>BCS</u> and associated <u>SCL</u>, but failed to include the process for identification, classification, and response to Cyber Security Incidents	Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement mitigation for the introduction of malicious code for <u>TCA</u> managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (<u>Requirement R2</u>)	according to Requirement R2, Attachment 1, Section 4. (<u>Requirement R2</u>) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES-Cyber Systems~~ <u>BCS</u> and <u>associated SCI</u> but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to	the introduction of malicious code for <u>TCA</u> managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (<u>Requirement R2</u>) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES-Cyber System~~ <u>BCS</u> according to Requirement R2, Attachment 1, Section 5.3. (<u>Requirement R2</u>)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				document mitigation for the introduction of malicious code for <u>TCA</u> managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (<u>Requirement</u> R2)		
R3	Operations Planning	Medium	The Responsible Entity has identified	The Responsible Entity has identified	The Responsible Entity has identified by name a	The Responsible Entity has not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	identified, by name, a CIP Senior Manager. OR 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. (Requirement 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	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	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	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. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (Requirement R4)	change in less than 50 calendar days of the change. (Requirement R4)	change. (Requirement R4)	OR 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 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ [See "Project 2016-02 Virtualization Implementation Plan."](#)

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.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact ~~BES-Cyber Systems~~ BCS.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	

Version	Date	Action	Change Tracking
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
<u>9</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES-Cyber Systems~~BCS or their associated SCI

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~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES-Cyber Systems~~BCS 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~~BCS within the asset, (2) the asset or the locations of the SCI hosting low impact BES Cyber Assets within the asset, and (3) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact ~~BES-Cyber System(s)~~BCS or its associated SCI identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

- 3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
 - i. between a low impact ~~BES-Cyber System(s)~~BCS and a ~~Cyber Asset(s)~~system(s) outside the asset containing low impact ~~BES-Cyber System(s)~~BCS;
 - ii. between SCI hosting a low impact BCS and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS;
 - iii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES-Cyber System(s)~~BCS or their associated SCI; and
 - iv. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).
- 3.2** Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES-Cyber System(s)~~BCS or their associated SCI, per Cyber Asset or VCA 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 Information Sharing and Analysis Center (E-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.

Section 5. Transient Cyber Asset TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems BCS or its associated SCI~~, through the use of ~~Transient Cyber Assets TCA~~ or Removable Media. The plan(s) shall include:

- 5.1 For ~~Transient Cyber Asset(s) TCA~~ managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per ~~Transient Cyber Asset TCA~~ 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.
- 5.2 For ~~Transient Cyber Asset(s) TCA~~ managed by a party other than the Responsible Entity, if any:
 - 5.2.1 Use one or a combination of the following prior to connecting the ~~Transient Cyber Asset TCA~~ to a low impact ~~BES Cyber System BCS or its associated SCI~~ (per ~~Transient Cyber Asset TCA~~ 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 the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or its associated SCI; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or its associated SCI.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES-Cyber Systems~~BCS or their associated SCI

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~~BCS or their associated SCI within the asset; and
 - b. The Cyber Asset(s) VCA, or SCI specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact ~~BES-Cyber Systems~~BCS, routable communication between a low impact ~~BES-Cyber System(s)~~BCS and ~~a Cyber Asset(s)~~ systems outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact ~~BES-Cyber System(s)~~BCS and ~~a Cyber Asset(s)~~ systems outside the asset containing low impact ~~BES-Cyber System(s)~~BCS or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. 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~~BCS).

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 Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or 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.

Section 5. Transient Cyber Asset~~TCA~~ and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 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~~TCA 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~~TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 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 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)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA 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~~TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, 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 the 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. 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-003-8, 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-003-8, 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 six 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-003-8, 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 may 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~~

~~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~~

~~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~~

~~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~~

~~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~~

~~For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~1.2.1 Cyber security awareness~~

~~Method(s) for delivery of security awareness~~

~~Identification of groups to receive cyber security awareness~~

~~1.2.2 Physical security controls~~

~~Acceptable approach(es) for selection of physical security control(s)~~

~~1.2.3 Electronic access controls~~

~~Acceptable approach(es) for selection of electronic access control(s)~~

~~1.2.4 Cyber Security Incident response~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Acceptable use of Transient Cyber Asset(s) and Removable Media~~

~~Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~

~~Method(s) to request Transient Cyber Asset and Removable Media~~

~~1.2.6 Declaring and responding to CIP Exceptional Circumstances~~

~~Process(es) to declare a CIP Exceptional Circumstance~~

~~Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~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:

~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included 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. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate “how” the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the 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 standard drafting team does not intend for Responsible Entities to be 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) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may 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 to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical 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.~~

~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

~~Monitoring as a physical security control can be used as a complement or an alternative to physical 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 standard drafting team's intent is that 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 of controlling physical access.~~

~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

Requirement R2, Attachment 1, Section 3—Electronic Access Controls

~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.~~

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR 61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles

away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

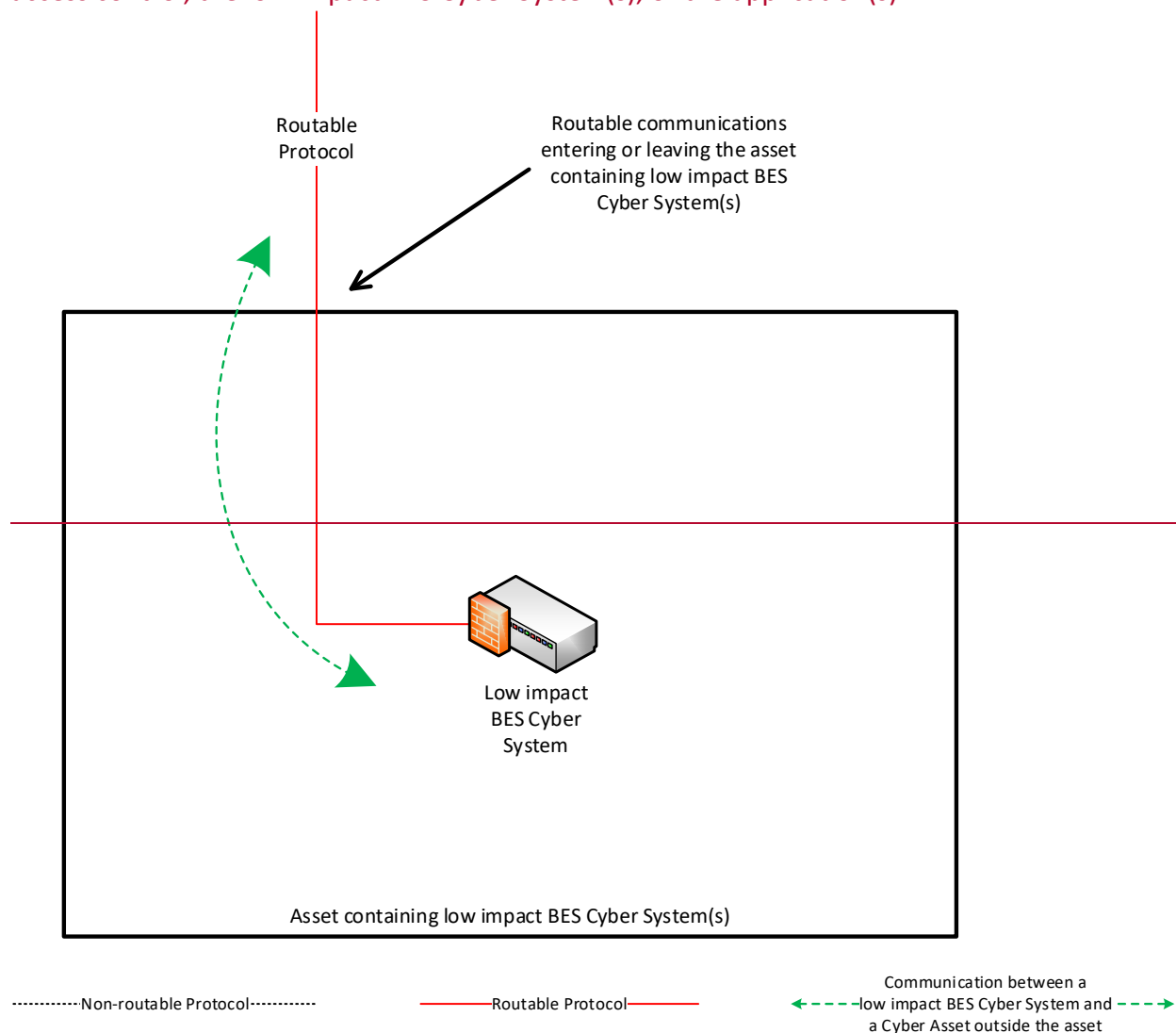
NOTE:

This is not an exhaustive list of applicable concepts.

The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1—Host-based Inbound & Outbound Access Permissions

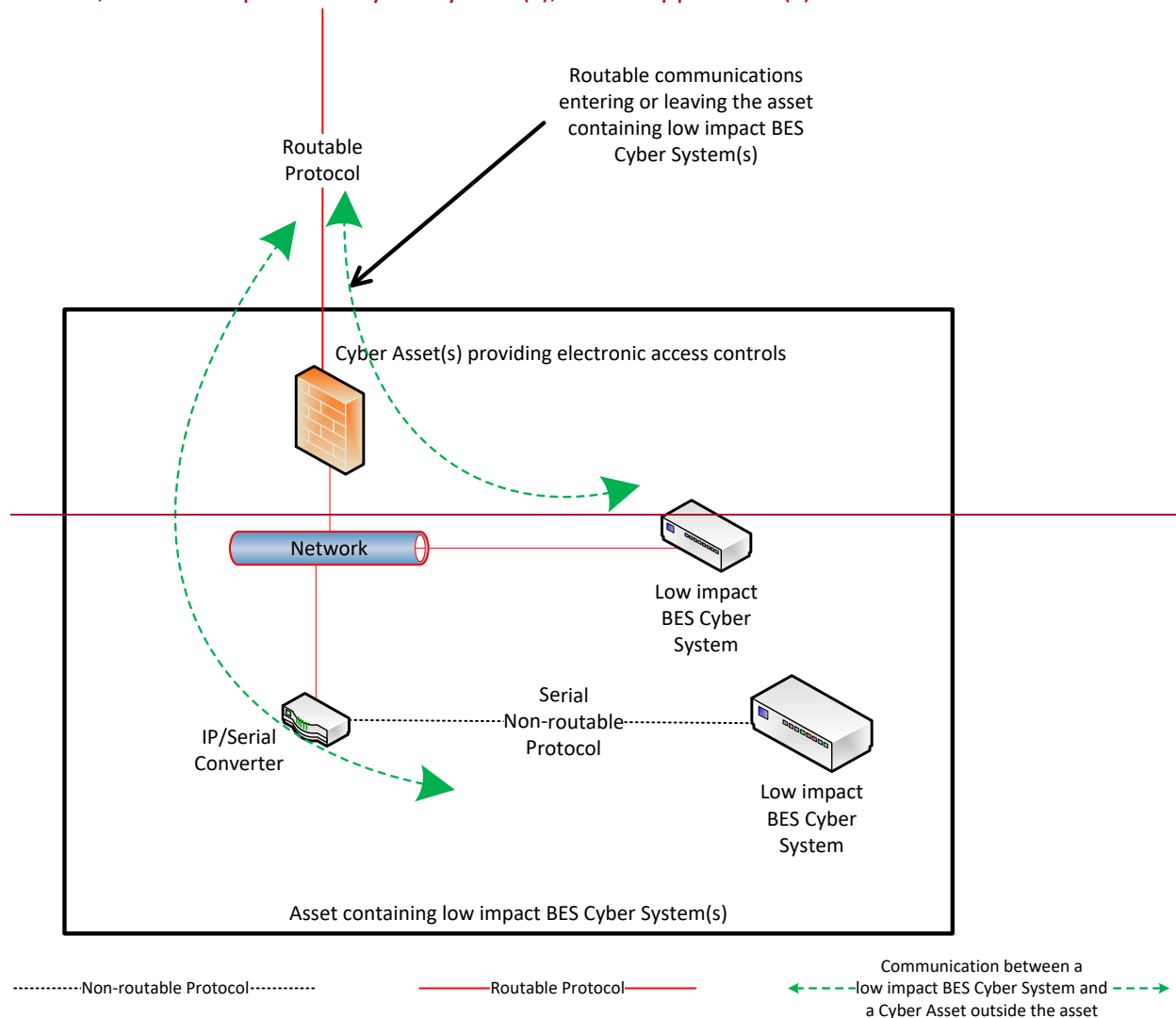
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

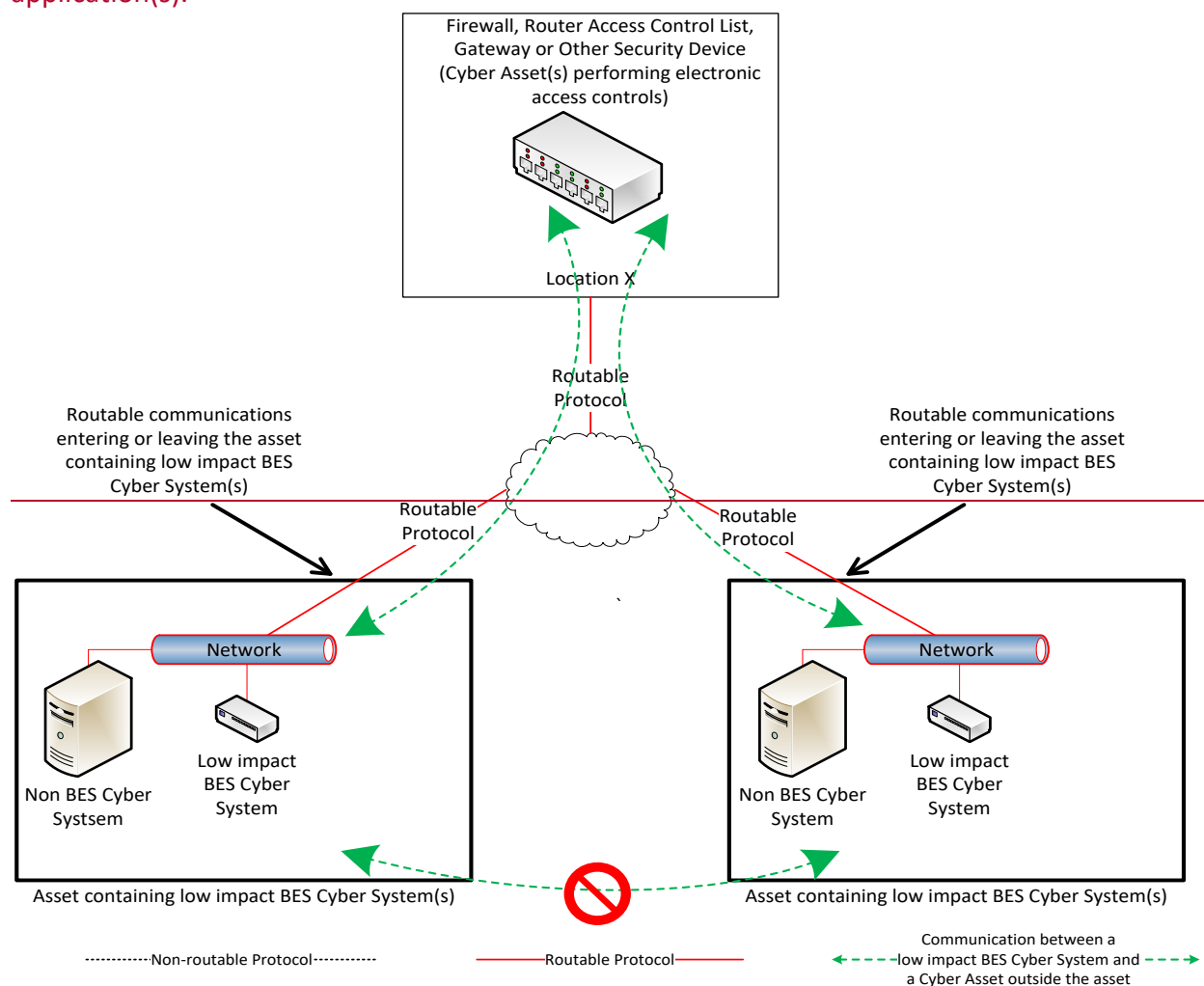
Reference Model 2—Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).

**Reference Model 2**

Reference Model 3—Centralized Network-based Inbound & Outbound Access Permissions

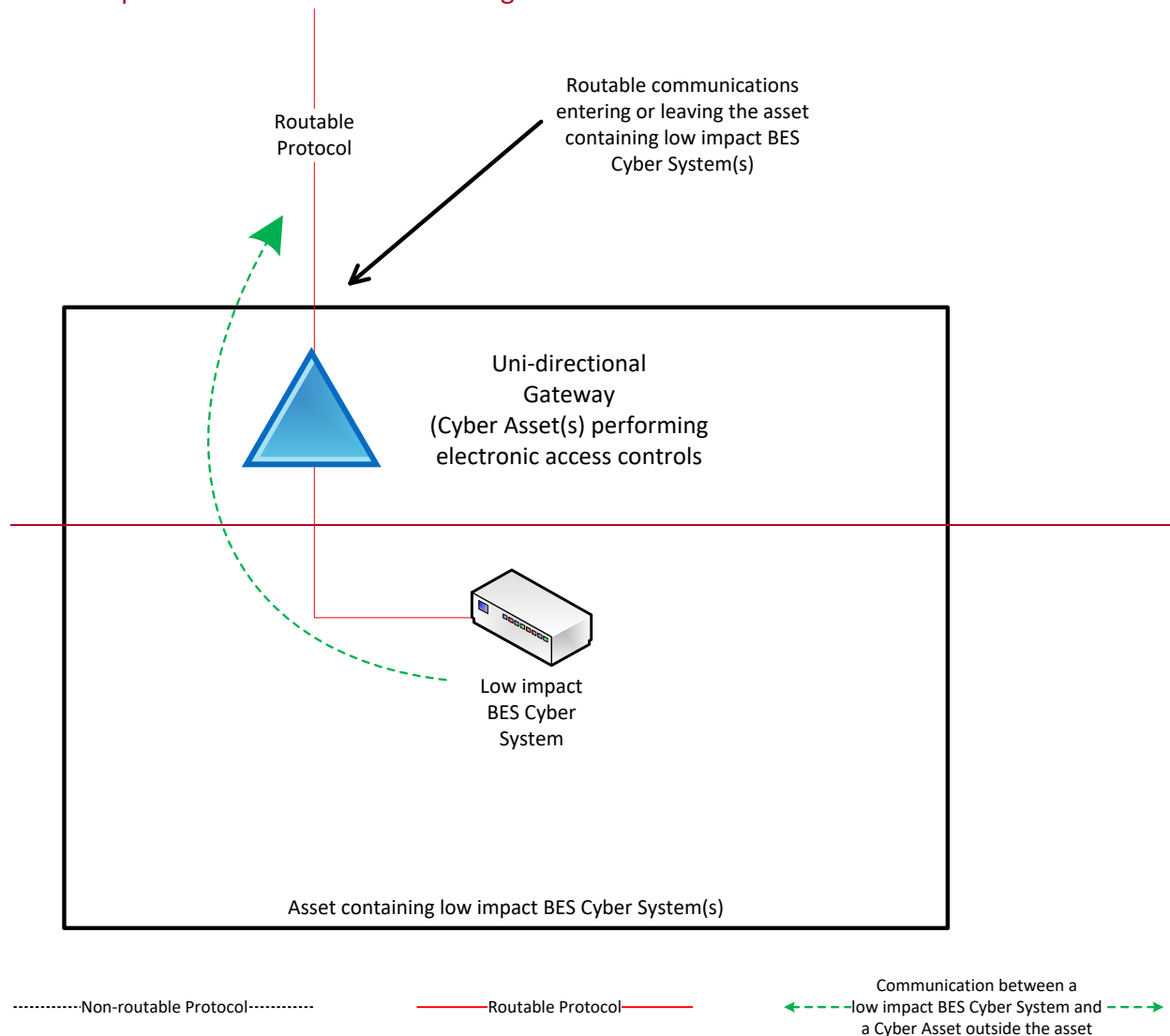
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at “Location X” to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4—Uni-directional Gateway

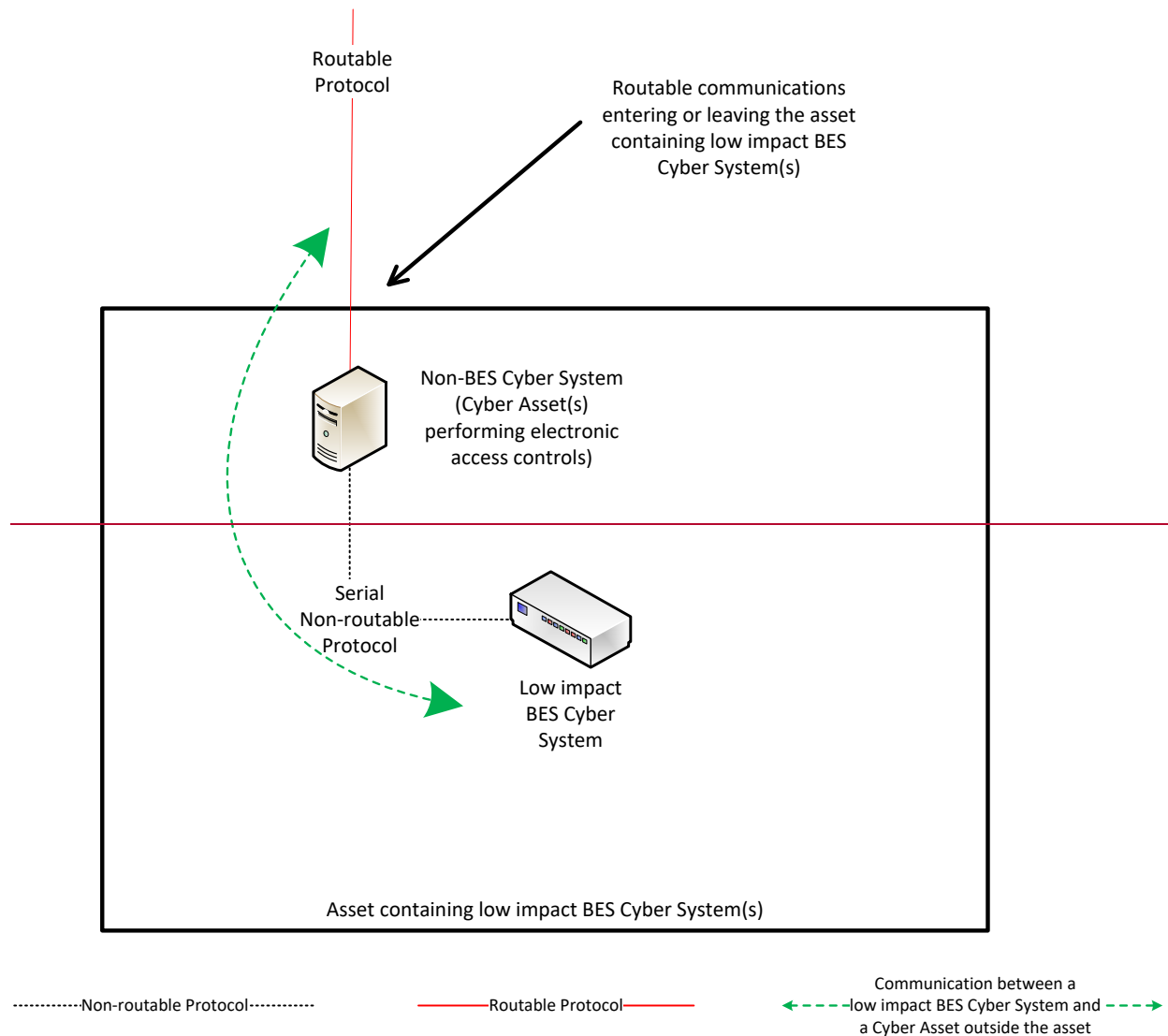
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5—User Authentication

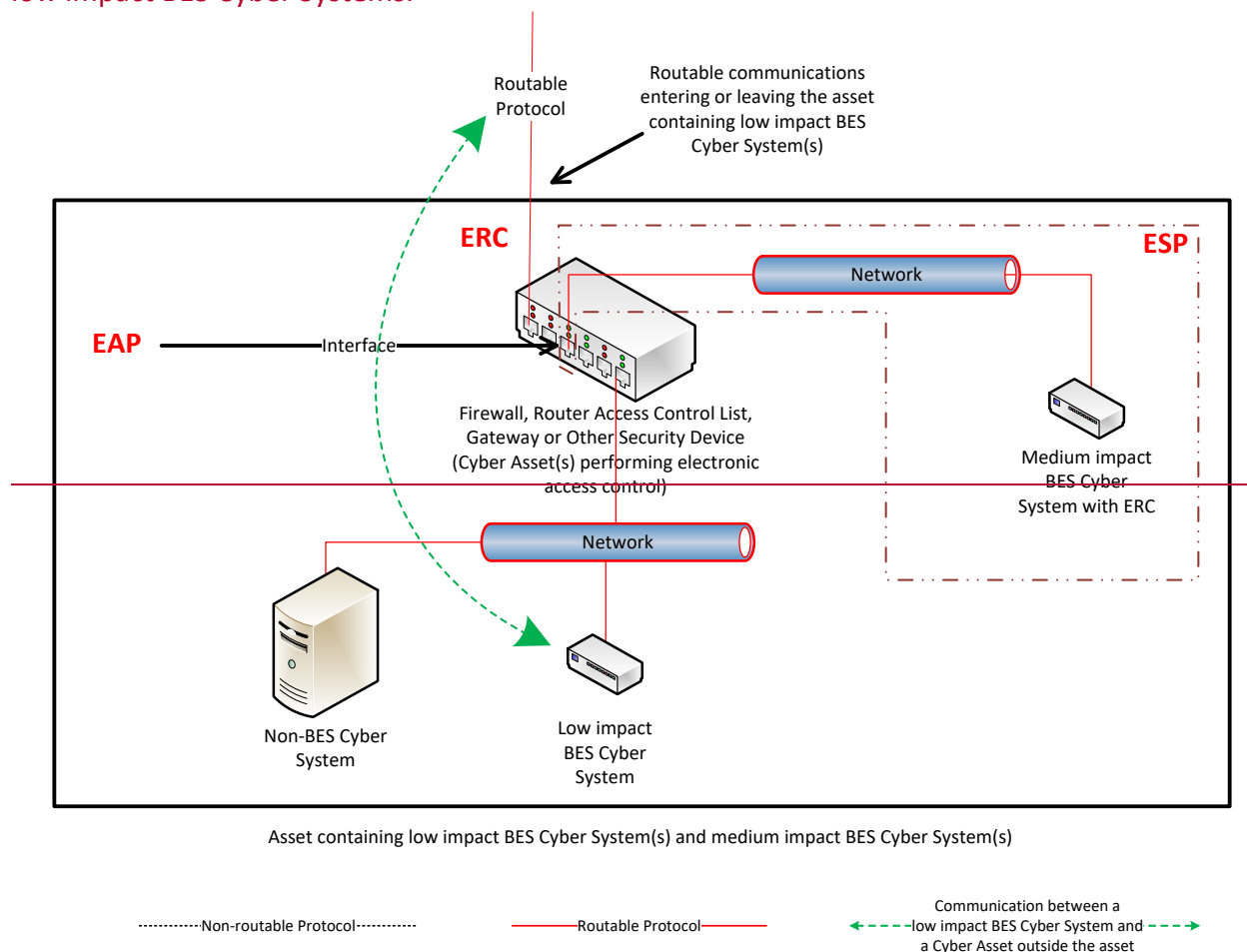
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user initiated interactive access.



Reference Model 5

Reference Model 7—Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions—as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



Reference Model 7

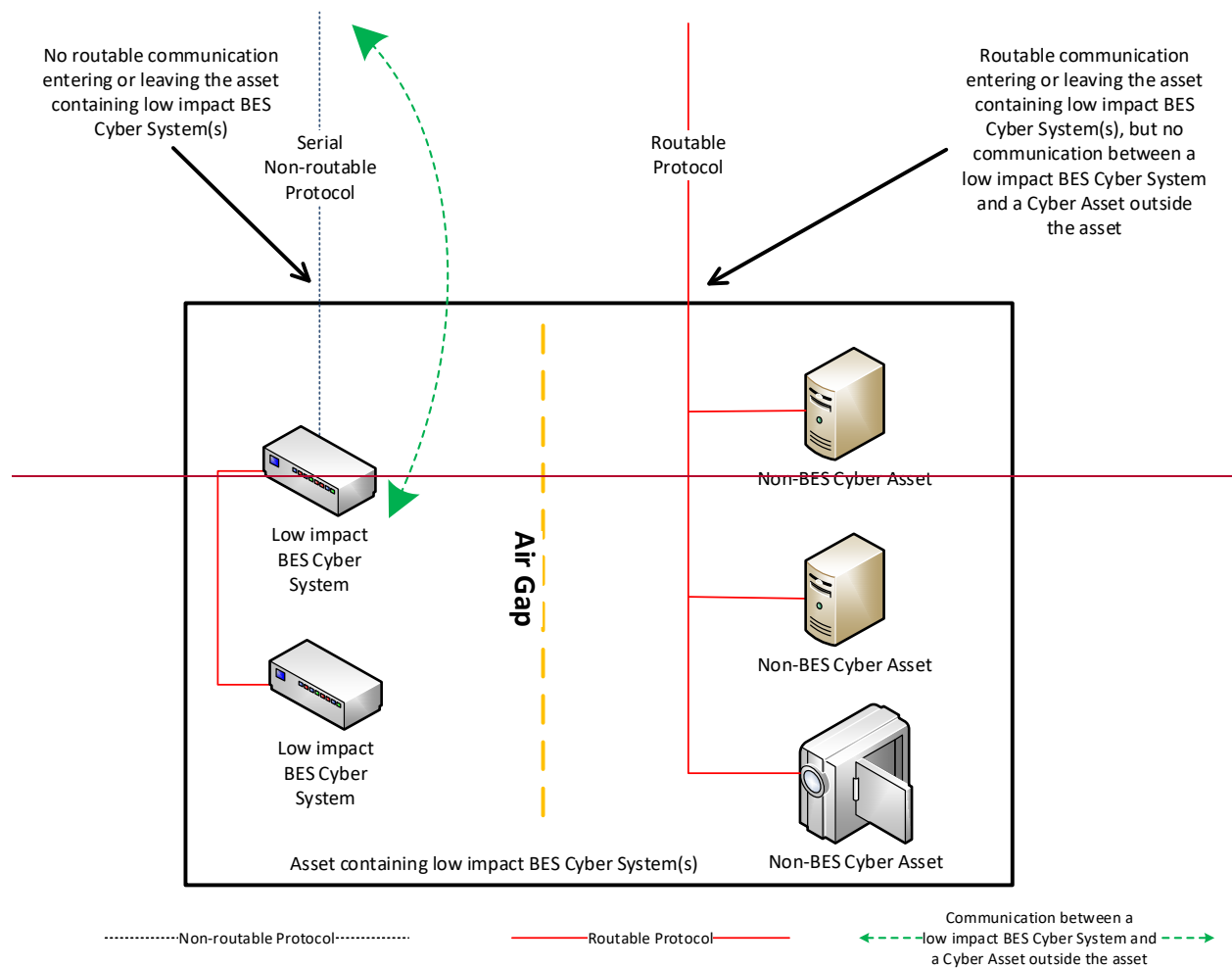
**Reference Model 8—Physical Isolation and Serial Non-routable Communications—
No Electronic Access Controls Required**

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an ‘air gap’, mitigates the need to implement the required electronic access controls;

The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.

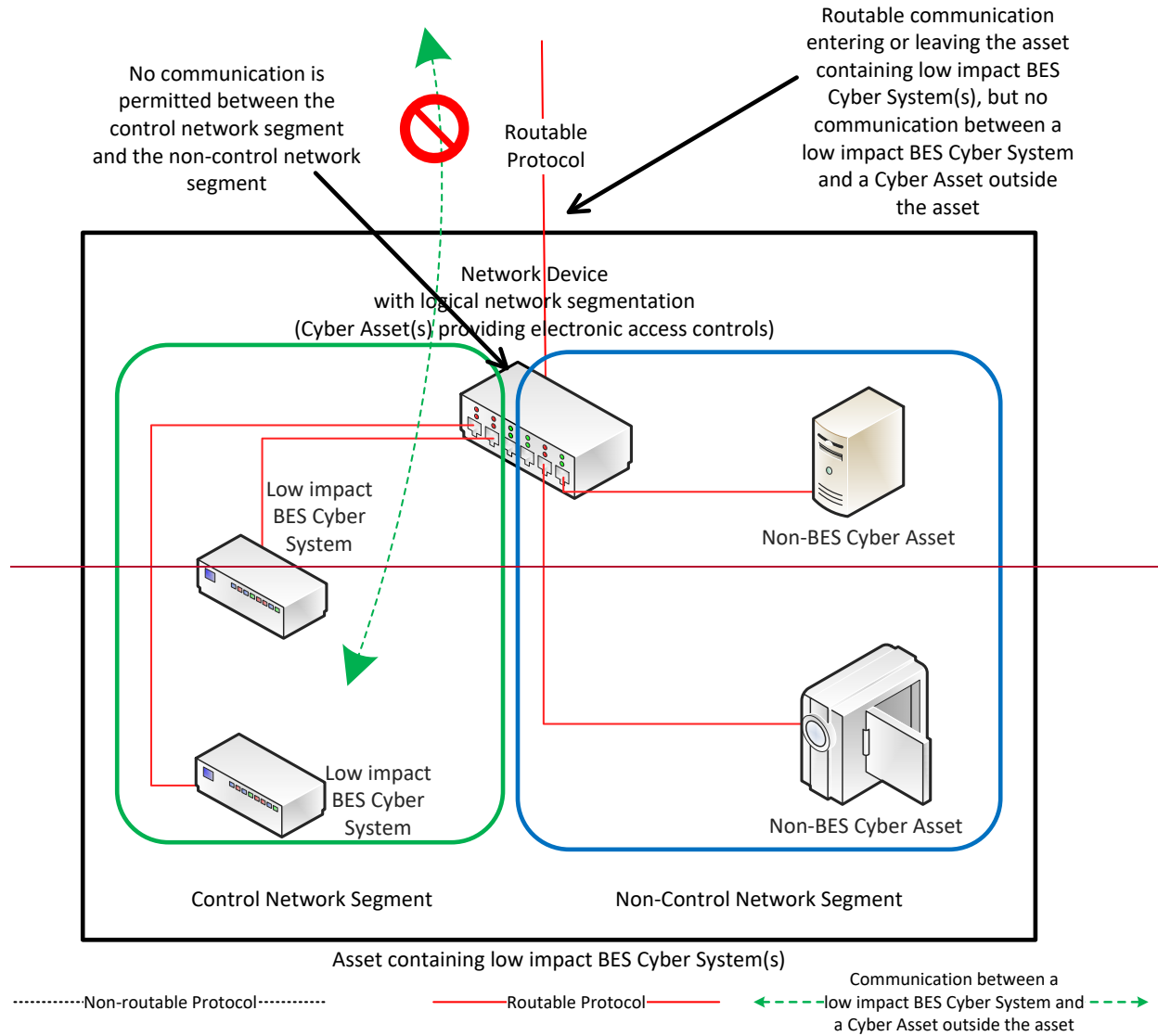
The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9—Logical Isolation—No Electronic Access Controls Required

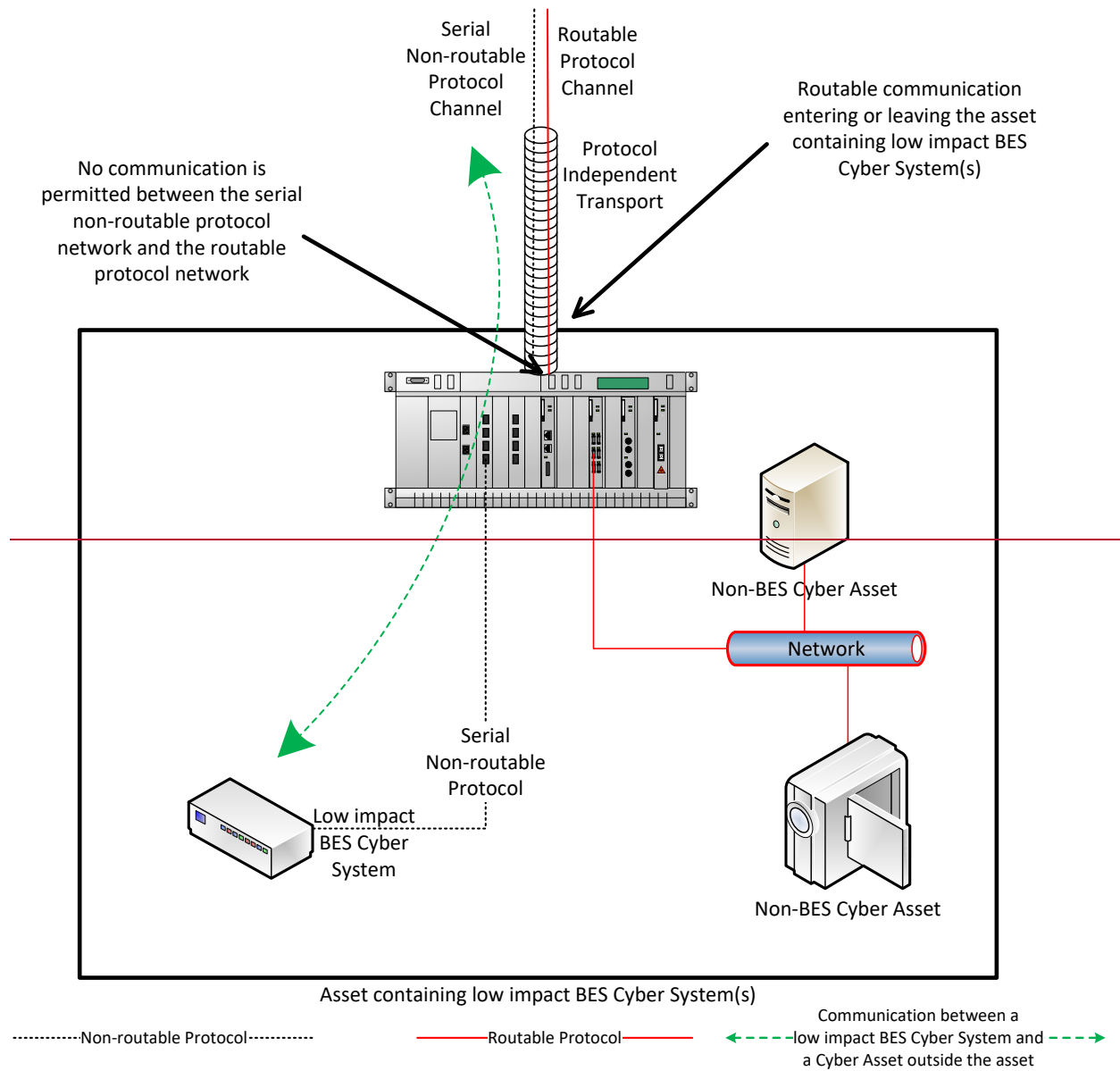
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10—Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network—No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide area network using a protocol independent transport that may carry routable and non-routable communication such as a Time Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

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.

Insufficient Access Controls

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.

A low impact BES Cyber System has a 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.

Dual homing or multiple network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

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 System(s), 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 R2, Attachment 1, Section 5—Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

~~Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~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 interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets.~~

~~Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~Examples of these temporarily connected devices include, but are not limited to:~~

~~Diagnostic test equipment;~~

~~Equipment used for BES Cyber System maintenance; or~~

~~Equipment used for BES Cyber System configuration.~~

~~To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

~~With the list of options provided in Attachment 1, 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 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 or BES Cyber Asset.~~

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

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 R2, Attachment 1, Section 5.1—Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: ~~Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code:

~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility 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 update the signatures or patterns and 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 risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System. When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code. If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Requirement R2, Attachment 1, Section 5.2—Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party’s security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of “prior to connecting the Transient Cyber Assets” is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~To facilitate these controls, Responsible Entities may 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 2014.⁴ 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 may 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.~~

⁴ <http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014>

Section 5.2.1: ~~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 method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.~~

Section 5.2.2: ~~The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.~~

Requirement R2, Attachment 1, Section 5.3—Removable Media

~~Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.~~

Section 5.3: ~~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 SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES 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 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, 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-003-8, 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.

Rationale:

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

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.~~

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 System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. 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 identified 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 System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.~~

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "...the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6...to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition...within one year of the effective date of this Final Rule."~~

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): “not used for time sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR 61850-90-5 R-GOOSE)”.

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to “the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.” The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to “...provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability.” Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

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.~~

~~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.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-~~7~~6
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 (BCS) by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting ~~BES Cyber Systems~~BCS.

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.~~4.1.5. Reliability Coordinator

~~4.1.7.4.1.6.~~ **Transmission Operator**

~~4.1.8.4.1.7.~~ **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-~~76~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication links between discrete Electronic Security Perimeters~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~ **4.2.3.3.** Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.4.2.3.4.~~ 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.

~~4.2.3.4.4.2.3.5.~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6.~~ Responsible Entities that identify that they have no ~~BES-Cyber-Systems~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“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. This concept was adapted 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.

5. Effective Dates: See “Project 2016-02 Virtualization” implementation Plan.~~” for CIP-004-6~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-~~76~~ 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-~~76~~ Table R1 – Security Awareness Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- ~~76~~ Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated SCI Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated SCI	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~~ <u>BCS or SCI</u> .	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 • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

- 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-~~76~~ 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-~~76~~ Table R2 – *Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-76 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. <u>Electronic Access Control or Monitoring System (EACMS)</u>; and 2. <u>Physical Access Control Systems (PACS)</u> Medium Impact ~~BES Cyber Systems~~ <u>BCS</u>, with External Routable Connectivity <u>(ERC) or Interactive Remote Access (IRA)</u>, and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI, with ERC or IRA, hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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 <u>(BCSI)</u> 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~~ <u>BCS and SCI</u>; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~ <u>BCS and SCI's</u> electronic interconnectivity and interoperability with other Cyber Assets <u>and VCA</u>, 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-004-76 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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, <u>VCA or SCI</u>, 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.

CIP-004-76 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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.

- 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~~ BCS or their associated SCI that collectively include each of the applicable requirement parts in CIP-004-~~76~~ 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-~~76~~ Table R3 – Personnel Risk Assessment Program and additional evidence to demonstrate implementation of the program(s).

CIP-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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-004-76 Table R3 — Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with <u>External Routable Connectivity</u> <u>ERC</u> or <u>IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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-year 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-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.3	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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.

CIP-004-~~76~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.4	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or Interactive Remote Access</u> <u>IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.5	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC- or ~~Interactive Remote Access~~ IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, <u>except during CIP Exceptional Circumstances, according</u> 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.

- 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-~~76~~ 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-~~76~~ 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-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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~~ <u>Information</u>BCSI.	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~~ <u>Information</u>BCSI.

CIP-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Verify at least once every 15 calendar months that access to the designated storage locations for ~~BES Cyber System Information~~BCSI, 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~~BCSI; 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.

- 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-~~76~~ 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-~~76~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- ~~76~~ Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> with ~~External Routable Connectivity~~<u>ERC</u> or ~~Interactive Remote Access~~<u>IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated EACMS or PACS.</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated EACMS or PACS.</u>	A process to initiate removal of an individual's ability for unescorted physical access and ~~Interactive Remote Access~~<u>IRA</u> 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-004-76 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	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-004-76 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	For termination actions, revoke the individual's access to the designated storage locations for ~~BES Cyber System Information~~BCSI, whether physical or electronic (unless already revoked according to Requirement R5 <u>Part 5.1</u>), 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~~BCSI associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-76 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: EACMS <u>SCI hosting High Impact BCS or their associated EACMS.</u>	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 applicable BES Cyber Assets~~systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.5	High Impact ~~BES Cyber Systems~~BCS and their associated: EACMS <u>SCI hosting High Impact BCS or their associated EACMS.</u>	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 Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~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~~**Violation Severity Levels**

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	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. (Requirement R1 Part 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. (Requirement R1 Part 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. (Requirement R1 Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Requirement R1 Part 1.1)
R2	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1)	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. (Requirement R2 Part 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. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2 Part R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in

R #	Violation Severity Levels (CIP-004-76)			
	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 the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical	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. (Requirement R2 Part 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. (Requirement R2 Part 2.3)	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. (Requirement R2 Part 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. (Requirement R2 Part 2.3)	Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 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. (Requirement R2 Part 2.2) OR 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. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)			
R3	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 one individual. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk	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 two individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized	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 three individuals. (Requirement 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.	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included 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. (Requirement 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

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (Requirement R3 Part 3.1 & Part 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	unescorted physical access but did not confirm identity for two individuals. (Requirement R3 Part 3.1 & Part 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 two individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	(Requirement R3 Part 3.1 & Part 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 three individuals. (Requirement R3 Part 3.2 & Part 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	or more individuals. (Requirement 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 four or more individuals. (Requirement R3 Part 3.1 & Part 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 or more individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	3.2.1 and 3.2.2 for one individual. (Requirement R3 Part 3.2 & Part 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 one individual. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not	electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (Requirement R3 Part 3.3 & Part 3.4) OR 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. (Requirement R3 Part 3.5)	three individuals. (Requirement R3 Part 3.3 & Part 3.4) OR 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. (Requirement R3 Part 3.5)	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. (Requirement R3 Part 3.3 & Part 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 years of the previous PRA completion date. (Requirement R3 Part 3.5)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)			
R4	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. (Requirement R4 Part 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. (Requirement R4 Part 4.2) OR	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. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account	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~~

R #	Violation Severity Levels (CIP-004-76)			
	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 Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR The Responsible Entity has implemented processes to verify	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 5% but less than (or equal to) 10% of its ~~BES Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System InformationBCSI~~ is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than	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 10% but less than (or equal to) 15% of its ~~BES Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System InformationBCSI~~ 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 InformationBCSI~~ storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)	~~InformationBCSI~~ is located. (<u>Requirement R4 Part 4.1</u>) 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. (<u>Requirement R4 Part 4.2</u>) 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 Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	that access to the designated storage locations for ~~BES Cyber System Information~~ BCSI is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyber System Information~~ BCSI storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)	(or equal to) 10% of its ~~BES Cyber System Information~~ BCSI storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)		The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~ BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~BES Cyber System Information~~ BCSI storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)
R5	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~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~ IRA upon a termination action or complete the removal within	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~ IRA upon a termination action or complete the removal within 24 hours of the termination action but did not	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or ~~BES Cyber System Information~~ BCSI storage locations. (<u>Requirement R5 Part R5</u>) OR

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Information BCSI~~, but for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 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. (Requirement R5 Part 5.4)	24 hours of the termination action but did not initiate those removals for one individual. (Requirement R5 Part 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 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. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more	initiate those removals for two individuals. (Requirement R5 Part 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 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. (Requirement R5 Part 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~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access IRA~~ upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (Requirement R5 Part 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. (Requirement R5 Part 5.2)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR 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. (<u>Requirement R5 Part 5.5</u>) OR The Responsible Entity has implemented one or more process(es) to determine and document	process(es) to revoke the individual's access to the designated storage locations for ~~BES-Cyber-System~~ ~~InformationBCSI~~ but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (<u>Requirement R5 Part 5.3</u>)	~~InformationBCSI~~ but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (<u>Requirement R5 Part 5.3</u>)	

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	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 circumstances. (Requirement R5 Part 5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents~~None.~~ See “Project 2016-02 Virtualization Implementation Plan.”**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.	

Version	Date	Action	Change Tracking
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
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact ~~BES Cyber Systems~~ <u>BCS</u> .
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — ~~Electronic Security Perimeter(s)~~BES Cyber System -Logical Isolation
2. **Number:** CIP-005-~~87~~
3. **Purpose:** To ~~manage electronic access to protect~~ BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication by specifying a controlled Electronic Security Perimeter to reduce the likelihood of misoperations or instability in the BES. in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns 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 Remedial Action Scheme (RAS) where the 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. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. 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 Section 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 RAS where the 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-005-~~87~~:

- 4.2.3.1. Cyber ~~Assets-systems~~ at Facilities regulated by the Canadian Nuclear Safety Commission.
- 4.2.3.2. Cyber ~~Assets-systems~~ associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).
- 4.2.3.3. ~~Cyber Ssystems~~ associated with communication links between Cyber Assets, ~~or~~ Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.
- 4.2.3.3.4.2.3.4. 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.
- 4.2.3.4.4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
- 4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~ BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “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. This concept was adapted 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.

- 5. **Effective Date:** See Project 2016-02 Virtualization Implementation Plan, ~~for Project 2019-03.~~

~~**Background:** Standard CIP-005 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. 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 Systems” column as described:

High Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

High Impact BES Cyber Systems with Dial-up Connectivity — Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

High Impact BES Cyber Systems with External Routable Connectivity — Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

Medium Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 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 Dial-up Connectivity — Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.

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.

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.

Electronic Access Points (EAP) — Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

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.

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.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-~~87~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-005-~~87~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: ~~1.~~ Protected Cyber Asset (PCA); ~~1-2.~~ Physical Access Control Systems (PACS) hosted on SCI; and ~~2-3.~~ Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: ~~1.~~ PCA; ~~1-2.~~ PACS hosted on SCI; and ~~2-3.~~ EACMS hosted on SCI	~~All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP~~ <u>Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).</u>	~~An e~~Examples of evidence may include, but is not limited to, ~~a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP~~documentation that includes the configuration of systems ~~that enforce electronic access control and logical isolation and document business need~~ such as: • <u>Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment);</u> • <u>SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration);-</u> <u>that enforces electronic access control and logical isolation and documents the business need.</u>

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~ Logical Isolation			
Part	Applicable Systems	Requirements	Measures
1.2	<u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>PCA;</u> <u>PACS; or</u> <u>EACMS</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> <u>PCA;</u> <u>PACS; or</u> <u>EACMS</u> <u>EACMS that perform logical isolation for a High Impact BCS</u> <u>EACMS that perform logical isolation for a Medium Impact BCS</u> <u>High Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> PCA <u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> PCA	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~ <u>Implement for applicable systems as follows:</u> <u>1.2.1. Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability.</u> <u>1.2.2. Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications.</u> <u>1.2.3. Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.</u>	~~An e~~<u>Examples</u> of evidence may include, but is not limited to, ~~network diagrams showing all external routable communication paths and the identified EAPs~~<u>documentation that includes the configuration of systems that enforce access control and logical isolation such as:</u> <u>Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment)</u> <u>Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems</u> <u>SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).</u>

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~ Logical Isolation			
Part	Applicable Systems	Requirements	Measures
1.3	<u>High Impact BCS and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>Medium Impact BCS connected to a network via routable protocol and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated:</u> <u>• PCA;</u> <u>• PACS; or</u> <u>• EACMS</u> ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	<u>Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of:</u> <u>• confidentiality and integrity controls (such as encryption), or</u> <u>• Physical controls that restrict access to the cabling and other nonprogrammable communication components,</u> <u>excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).</u> ~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of e~~Evidence may include, but is not limited to, <u>architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption)</u>~~a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~

CIP-005- ~~87~~ Table R1 – ~~Electronic Security Perimeter~~ Logical Isolation			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. <u>PCA;</u> 2. <u>PACS hosted on SCI; and</u> ~~4.~~3. <u>EACMS hosted on SCI</u> Medium Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. <u>PCA;</u> 2. <u>PACS hosted on SCI; and</u> 3. <u>EACMS hosted on SCI</u> <u>SCI with Dial-up Connectivity hosting High or Medium Impact BCS or their associated:</u> • <u>PCS;</u> • <u>PACS; or</u> • <u>EACMS</u>	~~Where technically feasible, p~~Perform authentication when establishing Dial-up Connectivity with applicable ~~Cyber Assets~~systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-~~87~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.5	<u>High Impact BCS and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>Medium Impact BCS at Control Centers and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> <u>• PCA;</u> <u>• PACS, or</u> <u>• EACMS</u> ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for~~ Detecting known or suspected malicious <u>Internet Protocol (IP)</u> communications ~~for both inbound and outbound communications~~<u>entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.</u>	An example of evidence may include, but is not limited to, documentation that malicious <u>Internet Protocol (IP)</u> communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

- R2.** For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the ~~Each~~ Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in CIP-005-~~87~~ Table R2 –Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M2.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in CIP-005-~~87~~ Table R2 –Remote Access Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~87~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~Interactive Remote Access (IRA) and their associated: • <u>PCA</u> <u>SCI with IRA hosting High or Medium Impact BCS or their associated:</u> • <u>PCA;</u> • <u>PACS; or</u> • <u>EACMS;</u> <u>Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PCA;</u> • <u>PACS; or</u> • <u>EACMS</u>	<u>Ensure that authorized IRA is through an Intermediate System.</u> ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams, ~~or~~ architecture documents, <u>or Management Systems reports that show all IRA is through an Intermediate System.</u>
2.2	<u>Intermediate Systems used to access applicable systems of Part 2.1</u>	<u>Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.</u>	An example of evidence may include, but is not limited to, architecture documents detailing where ~~encryption~~ <u>confidentiality and</u>

CIP-005-~~87~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
	~~High Impact BES Cyber Systems and their associated:~~ ~~1. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~	<u>integrity controls</u> initiates and terminates.
2.3	<u>Intermediate Systems used to access applicable systems of Part 2.1</u> ~~High Impact BES Cyber Systems and their associated:~~ ~~2. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~3. PCA~~	Require multi-factor authentication ~~for all Interactive Remote Access sessions~~<u>to the Intermediate System.</u>	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-87 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.4	High Impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with vendor remote access ~~External Routable Connectivity~~ and their associated: • PCA <u>SCI with vendor remote access hosting High or Medium Impact BCS or their associated:</u> • <u>PCA</u> <u>Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PCA</u>	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-~~87~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.5	High Impact ~~BES Cyber Systems~~BCS <u>with vendor remote access</u> and their associated: - PCA Medium Impact ~~BES Cyber Systems~~BCS with <u>vendor remote access</u>~~External Routable Connectivity~~ and their associated: - PCA <u>SCI with vendor remote access hosting High or Medium Impact BCS or their associated:</u> - PCA <u>Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated:</u> - PCA	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access IRA~~ and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the method(s) used to disable active vendor remote access (including ~~Interactive Remote Access IRA~~ and system-to-system remote access.), ~~such as: Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~

CIP-005-87 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
<u>2.6</u>	<u>Intermediate Systems used to access applicable systems of Part 2.1</u>	<u>Implement for applicable systems as follows:</u> <u>2.6.1.</u> <u>Restrict Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI.</u> <u>2.6.2.</u> <u>Permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.</u>	<u>Examples of evidence may include, but is not limited to, documentation that includes the following:</u> • <u>Configuration showing that the CPU and memory can only be shared with other IS.</u> • <u>Configuration showing how communications are controlled between the IS and applicable systems.</u>

- R3.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-~~7-8~~ Table R3 –Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M3.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in CIP-005-~~7-8~~ Table R3 – Vendor Remote Access Management for EACMS and PACS and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005- ~~87~~ Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~ BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~ BCS with External Routable Connectivity (ERC) <u>SCI hosting EACMS or PACS associated with High or Medium impact BCS</u> <u>Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS</u>	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~ BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~ BCS with External Routable	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include

CIP-005-~~87~~ Table R3 – Vendor Remote Access Management for EACMS and PACS

Part	Applicable Systems	Requirements	Measures
	~~Connectivity~~ ERC <u>SCI hosting EACMS or PACS associated with High or Medium impact BCS</u> <u>Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS</u>		terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

- 1.1. Compliance Enforcement Authority:** “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.
- 1.2. Evidence Retention:** The following evidence retention period(s) 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 applicable 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 applicable entity shall retain evidence of each requirement in this standard for three calendar years.
 - If an applicable 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 Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting <u>known or suspected</u> malicious Internet Protocol (IP) communications <u>entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2</u> ~~for both inbound and outbound communications.~~ (1.5)	The Responsible Entity did not document one or more processes for CIP-005-~~78~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation. (Requirement R1) OR The Responsible Entity did not <u>permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications.</u> ~~have all applicable Cyber Assetssystems connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). protected by logical isolation~~ (Requirement R1 Part 1.1) OR <u>The Responsible Entity did not protectimplement, for</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability the Management Systems or Management Interfaces or applicable systems per Requirement R1, Part 1.2 External Routable Connectivity through the ESP was not through an identified EAP. (Requirement R1 Part 1.2.1)</u> <u>OR</u> <u>The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>all other communications.</u> <u>(Requirement R1 Part 1.2.2)</u> <u>OR</u> <u>The Responsible Entity did</u> <u>not implement, for</u> <u>applicable systems, a</u> <u>method for denying</u> <u>communications from BCS</u> <u>and their associated PCAs to</u> <u>the Management Interfaces</u> <u>and Management Systems,</u> <u>per system capability</u> <u>(Requirement R1 Part 1.2.3)</u> <u>OR</u> <u>The Responsible Entity did</u> <u>not implement a method to</u> <u>protect the data traversing</u> <u>communication links, where</u> <u>the logical isolation spans</u> <u>multiple Physical Security</u> <u>Perimeters, through the use</u> <u>of confidentiality and</u> <u>integrity controls (such as</u> <u>encryption); or physical</u> <u>controls that restrict access</u> <u>to the cabling and other</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~nonprogrammable communication components protect confidentiality and integrity of the data traversing communications links per Requirement R1, Part 1.3. The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (Requirement R1 Part 1.3)~~ OR The Responsible Entity did not perform authentication when establishing ~~D~~ ial-up ~~e~~ Connectivity with the applicable ~~Cyber Assets~~ systems, where technically feasible. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3;	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3;

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement Parts 2.1 through 2.3.		OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.4</u>); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.5</u>).	OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.4</u>) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.5</u>). OR <u>The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>system capability</u> <u>(Requirement R2 Part 2.6.1)</u> OR <u>The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).</u>
R3.	The Responsible Entity did not document one or more processes for CIP-005- ~~87~~ Table R3 – Vendor Remote Access Management for EACMS and PACS. <u>(Requirement R3)</u>	The Responsible Entity had method(s) as required by Part 3.1 for EACMS <u>and SCI</u> <u>and -Management Modules of SCI</u> but did not have a method to determine authenticated vendor-initiated remote connections for PACS <u>(Requirement R3 Part 3.1)</u> . OR The Responsible Entity had method(s) as required by	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. <u>(Requirement R3)</u> OR The Responsible Entity had method(s) as required by Part 3.1 for PACS <u>and SCI</u> <u>and Management Modules of SCI</u> but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for CIP-005- ~~78~~ Table R3 – Vendor Remote Access Management for EACMS and PACS. <u>(Requirement R3)</u> OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 <u>(Requirement R3)</u> .

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Part 3.2 for EACMS, ~~and SCI~~ <u>and Management Modules of SCI</u> but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (<u>Requirement R3 Part 3.2</u>).	connections for EACMS (<u>Requirement R3 Part 3.1</u>). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS, ~~and SCI~~ <u>and Management Modules of SCI</u> but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (<u>Requirement R3 Part 3.2</u>). <u>OR</u> <u>The Responsible Entity had method(s) as required by Part 3.1 for PACS and ~~and~~ EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).</u>	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>OR</u> <u>The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).</u>	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.” for Project 2019-03
- CIP-005-~~87~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	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-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
<u>8</u>	<u>TBD</u>	<u>Virtualization modifications and ERC/IRA</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems
2. **Number:** CIP-006-~~76~~
3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems ~~(BCS)~~ against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns 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**~~~~**4.1.64.1.5 Reliability Coordinator**~~~~**4.1.74.1.6 Transmission Operator**~~~~**4.1.84.1.7 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-006-~~76~~:

4.2.3.1 Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.3.2~~ Cyber ~~Assets-systems~~ associated with communication ~~networks~~ and data communication links ~~between discrete Electronic Security Perimeters~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.24.2.3.3~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.34.2.3.4~~ 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.

~~4.2.3.44.2.3.5~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.54.2.3.6~~ Responsible Entities that identify that they have no ~~BES Cyber Systems~~ BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. “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. This concept was adapted 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.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan”

6. Background:

~~Standard CIP-006 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. 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 without External Routable Connectivity**—Only applies to medium impact BES Cyber Systems without External Routable Connectivity.~~

~~**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.~~

~~**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.~~

~~**Locally mounted hardware or devices at the Physical Security Perimeter**—Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-~~76~~ Table R1 – *Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*.
- M1.** Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-~~76~~ Table R1 – *Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-76 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> without External Routable Connectivity (<u>ERC</u>) <u>SCI without ERC hosting Medium Impact BCS</u> Physical Access Control Systems (PACS) associated with: • High Impact ~~BCS~~ <u>BES Cyber Systems</u>, or • <u>Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with External Routable Connectivity</u> <u>ERC</u> • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-76 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.2	Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	~~Where technically feasible, u~~ Utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, <u>per system capability</u> .	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.5	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident ~~R~~esponse ~~P~~lan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.6	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS, or • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.7	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS, or • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • <u>SCI hosting High Impact BCS or their associated EACMS or PCAs; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident ~~R~~ <u>r</u> esponse ~~P~~ <u>p</u> lan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.8	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated</u> • <u>EACMS; or</u> • <u>PCA</u>	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, <u>except during CIP Exceptional Circumstances</u>.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-76 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.9	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, <u>except during CIP Exceptional Circumstances</u>.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1—Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.10	High Impact BES Cyber Systems and their associated: - PCA Medium Impact BES Cyber Systems at Control Centers and their associated: - PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: - encryption of data that transits such cabling and components; or - monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or - an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

- R2.** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-~~76~~ Table R2 – Visitor Control Program. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*
- M2.** Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in CIP-006-~~76~~ Table R2 – Visitor Control Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~76~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~<u>BCS</u> with <u>External Routable Connectivity</u><u>ERC</u> and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, ~~except during CIP Exceptional Circumstances.~~	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-76 Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-~~76~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

- R3.** Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-~~76~~ *Table R3 – Maintenance and Testing Program*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
- M3.** Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in CIP-006-~~76~~ *Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-76 Table R3 – Physical Access Control System Maintenance and Testing Program

Part	Applicable Systems	Requirement	Measures
3.1	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS, ~~or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact ~~BES Cyber Systems~~BCS, ~~or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

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 Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Violation Severity Levels (CIP-006- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (Requirement R1 Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6)

R #	Violation Severity Levels (CIP-006-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption,~~

R #	Violation Severity Levels (CIP-006- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Requirement R2 Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact.

R #	Violation Severity Levels (CIP-006-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (Requirement R3 Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (Requirement R3 Part 3.1)

R #	Violation Severity Levels (CIP-006- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents~~None.~~ See [“Project 2016-02 Virtualization Implementation Plan”](#)**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

Version	Date	Action	Change Tracking
			other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes and CEC language added</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-~~76~~
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (~~BCS~~) 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

~~4.1.54.1.4~~ Interchange Coordinator or Interchange Authority

~~4.1.64.1.5~~ Reliability Coordinator

4.1.74.1.6 Transmission Operator**4.1.84.1.7 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-~~67~~:

4.2.3.1 Cyber Assets-systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets-systems associated with ~~communication networks and data~~ communication links ~~between discrete~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI). Electronic Security Perimeters.

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.24.2.3.4~~ 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.

~~4.2.3.34.2.3.5~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6~~ Responsible Entities that identify that they have no ~~BES Cyber Systems~~ BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. “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. This concept was adapted 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.

5. Effective Dates:

See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-007-76.~~

~~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

- 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 – System Hardening~~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 – System Hardening~~Ports and Services~~ and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R1— ~~Ports and Services~~ System Hardening			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, Enable only~~ logical-network accessible ~~ports-services~~ that have been determined to be needed by the Responsible Entity, ~~(or~~ <u>logical network accessible ports if unable to determine service</u>, including port ranges ~~or-services~~ where needed to handle dynamic ports), <u>per system capability</u>. -If a ~~device-system~~ has no provision for disabling or restricting <u>network accessible services (or logical ports)</u> ~~on the device~~ then those ~~ports services (or logical 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, ~~- policy~~, or other ~~device level~~ mechanisms that only allow needed ports and deny all others.

1.2	High Impact ~~BES Cyber Systems~~BCS and their associated ~~PCA~~; and ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated ~~PCA~~; and ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ <u>SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA</u> <u>Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers</u>	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.
	<u>SCI hosting High or Medium Impact BCS or their associated:</u>	<u>Enable only services that have been determined to be needed by the</u>	<u>Examples of evidence may include, but are not limited to:</u>

CIP-007-76 Table R1— ~~Ports and Services~~ System Hardening			
Part	Applicable Systems	Requirements	Measures
<u>1.3</u>	• <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	<u>Responsible Entity, per system capability.</u>	• <u>Documentation of implemented hardening guidelines</u> • <u>Configuration management reporting</u> <u>that demonstrates the need for all enabled services.</u>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ 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-~~76~~ Table R2 – Security Patch Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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 <u>for systems for applicable Cyber Assets</u> 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-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA;~~and~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA;~~and~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.4	High Impact ~~BES-Cyber Systems~~BCS 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 <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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.

- R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R3 – Malicious Code ~~Protection~~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-~~76~~ Table R3 – Malicious Code ~~Protection~~Prevention and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R3 – Malicious Code ~~Protection~~ Prevention			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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, <u>white-listing</u> , <u>privileged introspection</u> , etc.).

CIP-007-76 Table R3 – Malicious Code ~~Protection~~ Prevention			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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.

CIP-007-76 Table R3 – Malicious Code ~~Protection~~ Prevention			
Part	Applicable Systems	Requirements	Measures
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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.

- R4.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ 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-~~76~~ Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Log <u>security</u> events, <u>per system capability, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)</u> for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, ~~at~~ 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~~BCS 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~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI with ERC hosting High Impact BCS or Medium Impact BCS with ERC or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS</u> • <u>EACMS; or</u> • <u>PCA</u>	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, ~~as~~^{at} a minimum, each of the following types of events, ~~(per system or 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.

4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	~~Where technically feasible,~~ Retain applicable <u>security</u> event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, <u>per system or asset capability</u>, 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.

CIP-007-76 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	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.

- R5.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ 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-~~76~~ Table 5 – System Access Controls and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-67 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated:	Have a method(s) to enforce authentication of interactive user access, <u>per system capability</u>~~where technically feasible~~.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-67 Table R5 – System Access Controls			
Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA <u>SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>		
5.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated:	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-007-67 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES-Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>		

CIP-007-76 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.3	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~ BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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-007-76 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Change known default passwords, per ~~system or 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-007-76 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 <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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 <u>system</u>~~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 <u>system</u>~~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-007-76 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 <u>SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated:</u> • <u>PACS;</u>	~~Where technically feasible, f~~or 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, <u>per system capability</u>.	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.

	• <u>EACMS; or</u> • <u>PCA</u>		

CIP-007-76 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 <u>SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated:</u>	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts; <u>or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.</u>	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.

	• <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>		

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 Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

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~~

~~Table of Compliance Elements~~**Violation Severity Levels**

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has implemented and documented processes for ~~Ports and Services~~ <u>System Hardening</u> but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (<u>Requirement R1 Part 1.2</u>)	The Responsible Entity has implemented and documented processes for determining necessary ~~System Hardening~~ <u>Ports and Services</u> ~~but, where technically feasible, but~~ had one or more unneeded ~~logical~~ network accessible ~~services ports~~ enabled. (<u>Requirement R1 Part 1.1</u>) <u>OR</u> <u>The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)</u>	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007- ~~76~~ Table R1. (<u>Requirement R1</u>)
R2	The Responsible Entity has documented and implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for patch	The Responsible Entity has documented or implemented one or more	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	process(es) to evaluate uninstalled released security 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. (Requirement R2 Part 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 35 calendar days but less than 50 calendar	management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 Part 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 sources identified. (Requirement R2 Part 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	process(es) for patch management but did not include any processes for installing cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 Part 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. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating	process(es) that included the applicable items in CIP-007-76 Table R2. (Requirement 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~~systems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days of the evaluation completion. (Requirement R2 Part 2.3)	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. (Requirement R2 Part 2.3)	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. (Requirement R2 Part 2.3)	or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (Requirement R2 Part 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. (Requirement R2 Part 2.4)
R3	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		used, the Responsible Entity did not address testing the signatures or patterns. (Requirement R3 Part 3.3)	threat of detected malicious code. (Requirement R3 Part 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. (Requirement R3 Part 3.3).	included the applicable items in CIP-007- ~~76~~ Table R3. (Requirement 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. (Requirement R3 Part 3.1)
R4	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	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	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)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007- ~~76~~ Table R4. (Requirement R4)

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (Requirement R4 Part 4.4)	calendar days of the prior review. (Requirement R4 Part 4.4)	but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (Requirement R4 Part 4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 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. (Requirement R4 Part 4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an	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. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (Requirement R4 Part 4.4)	
R5	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. (Requirement R5 Part 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. (Requirement R5 Part 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). (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-76 Table R5. (Requirement 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.

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			identification of the individuals with authorized access to shared accounts. (Requirement R5 Part 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. (Requirement R5 Part 5.5) 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	(Requirement R5 Part 5.1) 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. (Requirement R5 Part 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 known default passwords.

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 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 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. (Requirement R5 Part 5.6)	(Requirement R5 Part 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. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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 generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~ See Project 2016-02 Virtualization Implementation Plan.
- See Technical Rationale for CIP-007-7

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.	

Version	Date	Action	Change Tracking
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.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization modifications</u>	

~~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.~~

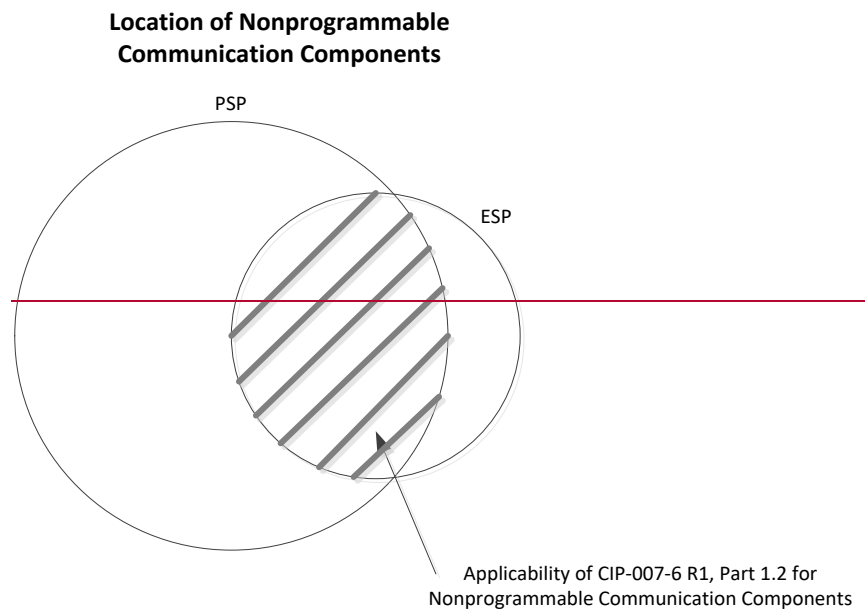
~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

- ~~• 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 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 010-2. The protections required here in CIP 007-6, 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.~~

Rationale:

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

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).~~

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.~~

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.~~

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.~~

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.

~~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.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-~~76~~
3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
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 Remedial Action Scheme where the Remedial Action Scheme 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 **Reliability Coordinator**

4.1.6 Transmission Operator**4.1.7 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 Remedial Action Scheme where the Remedial Action Scheme 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-008-~~76~~:

4.2.3.1 Cyber ~~Assets-systems~~ at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets-systems~~ associated with communication ~~networks and data communication~~ links ~~between discrete~~

Electronic Security Perimeters logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

4.2.3.24.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

4.2.3.34.2.3.4 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.

4.2.3.44.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BCS) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “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. This concept was adapted 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.

5. Effective Dates:

See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-008-76.~~

6. Background:

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 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 must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it 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 particular 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. 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 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** — Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications.
[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].
- M1.** Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications.

CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS.</u>	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: - A Reportable Cyber Security Incident; or - An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS</u>	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

- R2.** Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].
- M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS</u>	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations-based exercises.

CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS Medium Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> - EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS Medium Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> - EACMS	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	An example of 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 related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column.

- R3.** Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-~~76~~ Table R3 – *Cyber Security Incident Response Plan Review, Update, and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in CIP-008-~~76~~ Table R3 – *Cyber Security Incident Response Plan Review, Update, and Communication*.

CIP-008-76 Table R3 – Cyber Security Incident Response Plan
Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, ~~all of~~ the following: - Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; - Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and - Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

CIP-008-76 Table R3 – Cyber Security Incident Response Plan
Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: - Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and - Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

- R4.** Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),¹ or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column, unless prohibited by law, in accordance with each of the applicable requirement parts in CIP-008-~~76~~ Table R4 – Notifications and Reporting for Cyber Security Incidents. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M4.** Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column according to the applicable requirement parts in CIP-008-~~76~~ Table R4 – Notifications and Reporting for Cyber Security Incidents.

CIP-008- ~~76~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

¹ The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

CIP-008-76 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: - One hour after the determination of a Reportable Cyber Security Incident. - By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

CIP-008-76 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.3	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS</u>	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. 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. 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~~ Enforcement Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self Reporting~~
- ~~Complaint~~

~~1.4. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning	Lower	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the “Applicable Systems” column for Part 1.2. (Requirement R1 Part 1.2)
R2	Operations Planning Real-time Operations	Lower	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.2 occurs. (Requirement R2 Part 2.2)	calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.3. (Requirement R2 Part 2.3)
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any	The Responsible Entity has neither documented lessons learned nor documented the	The Responsible Entity has neither documented lessons learned nor documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3)	documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3) OR	absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the Cyber Security	absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	Operations Assessment	Lower	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.3 but failed to report on	Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column. (Requirement R4 Part R4)	Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1.			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ [See "Project 2016-02 Virtualization Implementation Plan."](#)

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	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-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems
2. **Number:** CIP-009-~~76~~
3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns 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 or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System 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**~~~~**4.1.6.4.1.5. Reliability Coordinator**~~~~**4.1.7.4.1.6. Transmission Operator**~~~~**4.1.8.4.1.7. 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 or Remedial Action Scheme~~RAS where the ~~Special Protection System 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-009-~~76~~:

4.2.3.1. Cyber ~~Assets~~systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~systems associated with communication ~~networks and data communication links between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~**4.2.3.3.** Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~**4.2.3.4.** 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.~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~75.1~~ identification and categorization processes.

4.3. “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. This concept was adapted 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.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan” ~~for CIP-009-76.~~

~~**6. Background:** Standard CIP-009 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 their documented processes, but they must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~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. 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 BES Cyber Systems located at a Control Center and 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 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

- R1.** Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-~~76~~ Table R1 – Recovery Plan Specifications. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*
- M1.** Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in CIP-009-~~76~~ Table R1 – Recovery Plan Specifications.

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS; or</u> • <u>EACMS</u>	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-76 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	One or more processes for the backup and storage of information required to recover ~~BES Cyber System~~<u>applicable system</u> functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber System~~<u>applicable system</u> functionality.

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.5	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	One or more processes to preserve data, per <u>Cyber Assets</u> system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

- R2.** Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-~~76~~ Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]
- M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in CIP-009-~~76~~ Table R2 – Recovery Plan Implementation and Testing.

CIP-009- ~~76~~ Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~<u>BCS</u> at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-~~76~~ Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	Test a representative sample of information used to recover ~~BES Cyber System~~ <u>applicable system</u> functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber System~~ <u>applicable system</u> functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-76 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~ BCS SCI hosting High Impact ~~BES Cyber Systems~~ BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

- R3.** Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-76 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in CIP-009-76 Table R3 – Recovery Plan Review, Update and Communication.

CIP-009-76 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers and their associated:</u> <u>PACS; or</u> <u>EACMS</u>	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: - Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; - Dated and revised recovery plan showing any changes based on the lessons learned; and - Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

CIP-009-76 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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 Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.4. Compliance Monitoring and Assessment Processes:~~

- ~~• Compliance Audits~~
- ~~• Self-Certifications~~
- ~~• Spot-Checking~~
- ~~• Compliance Investigations~~
- ~~• Self-Reporting~~
- ~~• Complaints~~

~~1.5. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in <u>Requirement R1</u> Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in <u>Requirement R1</u> Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for ~~BES Cyber Systems~~<u>applicable systems</u>. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~<u>applicable systems</u>, but the plan(s) does not address the conditions for activation in <u>Requirement R1</u> Part 1.1. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~<u>applicable systems</u>, but the plan(s) does not address three or more of the requirements in Parts <u>Requirement R1</u> 1.2 through 1.5.

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)	months between tests. (Requirement R2 Part 2.3)	The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)	
R3.	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2)	

R #	Violation Severity Levels (CIP-009- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			• Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See “Project 2016-02 Virtualization Implementation Plan.”

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.	

Version	Date	Action	Change Tracking
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-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

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 following guidelines are available to assist in addressing the required components of a recovery plan:~~

~~NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at~~

~~<http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf>~~

~~National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at~~

~~http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

~~Installation files and media;~~

~~Current backup tapes and any additional documented configuration settings;~~

~~Documented build or restoration procedures; and~~

~~Cross-site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not~~

~~required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

~~Periodic (e.g. daily or weekly) backup process—Review generated logs or job status reports and set up notifications for backup failures.~~

~~Non-periodic backup process—If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~

~~Data mirroring—Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~

~~Manual configuration information—Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

~~For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.~~

Requirement R2:

~~A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.~~

~~A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.~~

~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures.”~~

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

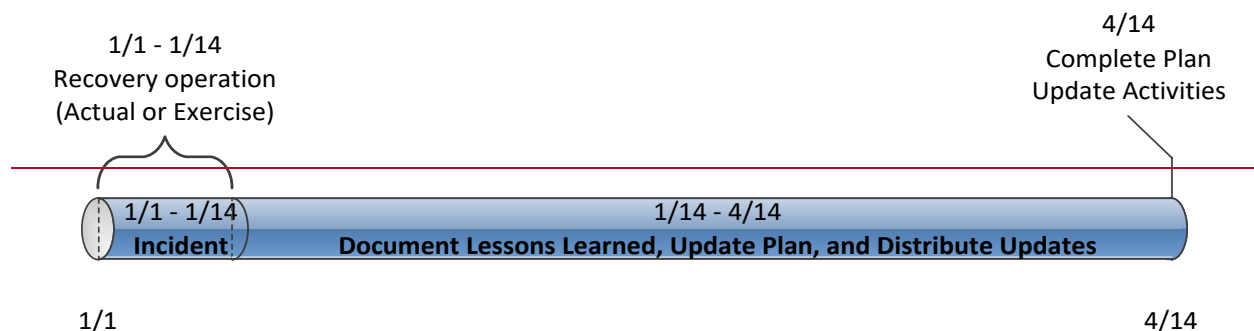


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

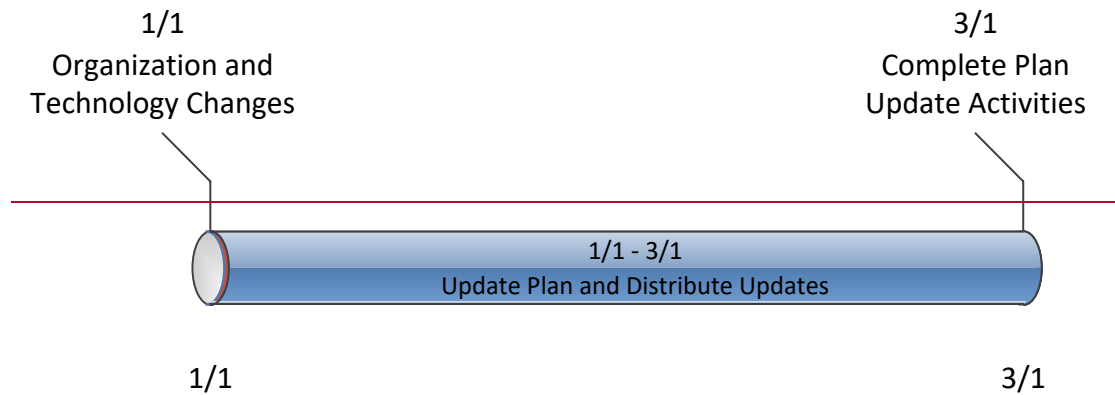


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

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

Rationale for Requirement R1:

~~Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

Rationale for Requirement R2:

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

Rationale for Requirement R3:

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — ~~Configuration~~ Change Management and Vulnerability Assessments
2. **Number:** CIP-010-~~54~~
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 Remedial Action Scheme (RAS) where the 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. Reliability Coordinator****4.1.6. Transmission Operator****4.1.7. 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 Section 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 RAS where the 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-010-54:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic~~

Security Perimeters logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCL.

4.2.3.2.4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

4.2.3.3.4.2.3.4. 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.

4.2.3.4.4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “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. This concept was adapted 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.

5. — Effective Date: See “Project 2016-02 Virtualization Implementation Plan.” for Project 2019-03.

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 identification and categorization processes.

Medium Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 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

- R1.** Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in CIP-010-54 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-010-54 Table R1 – ~~Configuration~~ Change Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 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 <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	~~Authorize changes to~~<u>Develop a baseline configuration, individually or by group, which shall include the following items:</u> 1.1.1. Operating system(s) ~~(including version)~~ or firmware ~~where no independent operating system exists~~ <u>or images used to derive operating systems or firmware;</u> 1.1.2. ~~Any e~~Commercially available or open-source application software ~~(including version)~~ <u>intentionally installed including Self-Contained Applications;</u> 1.1.3. ~~Any e~~Custom software installed <u>including Self-Contained Applications;</u> 1.1.4. Any logical network accessible ~~ports~~ <u>services, (or logical ports if unable to determine service);</u>	Examples of evidence may include, but are not limited to: • <u>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.</u> ~~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-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	<u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	~~and~~ <u>1.1.5. Any Security patches applied;</u> <u>1.1.6. SCI configuration that:</u> • <u>Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI;</u> • <u>-Enforces logical isolation between systems with different impact ratings hosted on SCI;</u> • <u>Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or</u> • <u>Enables or disables SCI services.</u>	
~~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:~~ ~~1. EACMS;~~	~~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~~

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	~~2. PACS; and~~ ~~3. PCA~~		~~change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~
~~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.~~
~~1.24~~	~~High Impact BES Cyber Systems~~ <u>BCS</u> and their associated: ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems~~ <u>BCS</u> and their associated: ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a each change that deviates from the existing baseline configuration to the items listed in Part 1.1:~~ ~~1.2.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;~~ ~~1.2.2. Following the change, verify that required cyber security controls determined in 1.24.1 are not~~	~~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-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	<u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>PACS;</u> <u>EACMS; or</u> <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> <u>PACS;</u> <u>EACMS; or</u> <u>PCA</u>	adversely affected; and <u>1.2.3.</u> Document the results of the verification.	
1.35	High Impact BCS <u>SCI hosting High Impact BCS</u>	~~Where technically feasible, for each change that deviates from the existing baseline configuration to the items listed in Part 1.1, per system capability:~~ <u>1.3.1.</u> Prior to implementing any change in the production environment, <u>except during a CIP Exceptional Circumstance</u>, test the changes in a test environment <u>that minimizes differences with the production environment</u> -or test the	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 the date of the test.

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
		changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and <u>1.3.2.</u> 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.	
1.64	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS	Prior to a change ~~that deviates from the existing baseline configuration~~ associated with ~~baseline items~~ <u>in Requirement</u> Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: <u>1.46.1.</u> Verify the identity of the software source; and <u>1.46.2.</u> Verify the integrity of the software obtained from the	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	<u>SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.</u> <u>Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.</u> Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.46: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	software source.	

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4.5 Table R2 – ~~Configuration Change~~ 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-010-4.5 Table R2 – ~~Configuration Change~~ Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R2 – ~~Configuration Change~~ Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for ~~unauthorized~~ changes to the ~~baseline configuration (as items~~ 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.

- R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-~~3-5~~ 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-~~3-5~~ Table R3 – *Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4.5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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-010-4.5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems <u>SCI hosting High Impact BCS.</u> <u>Management Modules of SCI hosting High Impact BCS.</u>	~~Where technically feasible, a~~At least once every 36 calendar months, <u>per system capability</u>: 3.2.1 Perform an active vulnerability assessment in a test environment <u>that minimizes differences with the production environment</u>, 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-010-4.5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BES Cyber Systems or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	<u>Perform an active vulnerability assessment prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability</u>~~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, <u>or</u> ~~and like replacements~~<u>deployments of the same type of Cyber Asset with</u> using a <u>baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset previously assessed configuration. The production environment does not include devices being actively remediated and logically isolated.</u>	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, <u>Virtual Cyber Asset, or Shared Cyber Infrastructure</u>) and the output of any tools <u>or Management Systems</u> used to perform the assessment.

3.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	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, <u>a report of Management System actions, or</u> 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).

- R4.** Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated SCI and 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

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) 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 applicable 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 applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable 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 Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a ~~configuration~~-change management process(es) that includes only four <u>or more</u> of the required ~~baseline~~-items listed in 1.1.1 through 1.1.65. (<u>Requirement R1 Part 1.1</u>)	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 1.1.65. (<u>Requirement R1 Part 1.1</u>)	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 1.1.65. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity has a process as specified in Part 1.64 to verify the identity of the software source (1.64.1) but does not have a process as specified in Part 1.64 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (<u>Requirement R1 Part 1.64.2</u>)	The Responsible Entity has not documented or implemented any ~~configuration~~-change management process(es). (<u>Requirement R1</u>) 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 1.1.65. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity does not have a <u>change management</u> process(es) that requires authorization ~~and documentation~~ of changes ~~that deviate from the existing baseline~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~configuration to items listed in 1.1.1-1.1.6. (Requirement R1 Part 1.12)~~ 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 that could be impacted by a change(s) that deviates from the existing ~~baseline~~ configuration. (Requirement R1 Part 1.42.1) OR The Responsible Entity has a process(es) to determine required security controls in

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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. (<u>Requirement R1 Part 1.42.2</u> & <u>Part 1.42.3</u>) 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 to the~~ configuration. (<u>Requirement R1 Part 1.53.1</u>) OR The Responsible Entity does not have a process to document the test results and, if using a test

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				environment, document the differences between the test and production environments. (Requirement R1 Part 1.53.2) OR The Responsible Entity does not have a process as specified in Part 1.64 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.64)
R2.	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 <u>the items described in</u> Requirement R1, Part 1.1.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~the baseline~~ at least once every 35 calendar days. (<u>Requirement R2 Part 2.1</u>)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~A~~applicable ~~s~~Systems, but has performed an active vulnerability assessment more than 36 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~a~~Applicable ~~s~~Systems, but has performed an active vulnerability assessment more than 39 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~a~~Applicable ~~s~~Systems, but has performed an active vulnerability assessment more than 42 months, but	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3</u>) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	less than 39 months, since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>)	less than 42 months, since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>)	less than 45 months, since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>)	documented active vulnerability assessment processes for ~~a~~ Applicable ~~s~~ Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable ~~BES Cyber S~~ systems, but did not perform the active vulnerability assessment ~~in a manner that models an existing baseline configuration~~ of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.3</u>)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES~~ ~~Cyber-S~~ 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. (<u>Requirement R3 Part 3.4</u>)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-45, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-45, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-45, Requirement R4,	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-45, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 1.1. (Requirement R4 Part 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-010-45, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	Attachment 1, Section 3. (Requirement 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, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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- ~~45~~ , Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (<u>Requirement</u> R4)	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- ~~45~~ , Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (<u>Requirement</u> R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”~~for Project 2019-03.~~
- CIP-010-~~4~~5 Technical Rationale

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.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	
<u>5</u>	<u>TBD</u>	<u>Virtualization modifications</u>	

CIP-010-54 - 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 prior to connecting to a ~~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-010-45 - 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.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-~~32~~
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) 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~~~~4.1.6.4.1.5.~~ Reliability Coordinator~~4.1.7.4.1.6.~~ Transmission Operator~~4.1.8.4.1.7.~~ 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-~~32~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic~~

~~Security Perimeters~~ logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCL.

~~4.2.3.2.4.2.3.3.~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.4.2.3.4.~~ 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.

~~4.2.3.4.4.2.3.5.~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6.~~ 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. “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. This concept was adapted 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.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-011-32.~~

~~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

- 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-~~32~~ 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-~~32~~ Table R1 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011- ~~32~~ Table R1 – Information Protection			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems <u>(BCS)</u> and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS.</u>	Method(s) to identify information that meets the definition of ~~BES Cyber System Information~~<u>BCSI</u>.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify ~~BES Cyber System Information~~<u>BCSI</u> from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~<u>BCSI</u> as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize ~~BES Cyber System Information~~<u>BCSI</u>; or • Repository or electronic and physical location designated for housing ~~BES Cyber System Information~~<u>BCSI</u> in the entity's information protection program.

CIP-011-~~32~~ Table R1 – Information Protection

Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Procedure(s) for protecting and securely handling ~~BES Cyber System Information~~<u>BCSI</u>, 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~~<u>BCSI</u>; or • Records indicating that ~~BES Cyber System Information~~<u>BCSI</u> is handled in a manner consistent with the entity's documented procedure(s).

- R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-~~32~~ 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-~~32~~ 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- ~~32~~ 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 <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS;</u> • <u>PACS; or</u> • <u>PCA</u>	<u>Method(s) 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 InformationBCSI from applicable systems prior to upon their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). outside another applicable systemthe Cyber Asset data storage media.</u>	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyber System InformationBCSI~~ 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 InformationBCSI~~.

CIP-011-~~32~~ 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 Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~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.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-011- ~~32~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a ~~BES Cyber System Information~~ BCSI protection program (<u>Requirement R1</u>).
R2.	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~~ BCSI from the BES Cyber Asset. (<u>Requirement R2 Part 2.1</u>)	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~~ BCSI from the BES Cyber Asset. (<u>Requirement R2 Part 2.2</u>)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011- ~~32~~ Table R2 – BES Cyber Asset Reuse and Disposal. (<u>Requirement R2</u>)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan. Guideline and Technical Basis (attached).”

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.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
<u>3</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

~~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 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.~~

Rationale

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

Rationale for Requirement R1:

~~The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

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.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security - Supply Chain Risk Management
2. **Number:** CIP-013-~~32~~
3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems and their associated 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 Remedial Action Scheme (RAS) where the 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.
 - 4.1.3. **Generator Operator**
 - 4.1.4. **Generator Owner**
 - 4.1.5. **Reliability Coordinator**
 - 4.1.6. **Transmission Operator**
 - 4.1.7. **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 RAS where the 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-013-~~32~~:

4.2.3.1. Cyber ~~Assets-systems~~ at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets-systems~~ associated with communication ~~networks and data communication-links between discrete Electronic Security Perimeters (ESPs)~~ logically isolated from, but not providing logical isolation for, BES Cyber Systems (BCS) or Shared Cyber Infrastructure (SCI).

~~4.2.3.3.~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. 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.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 Virtualization Implementation Plan."~~for Project 2019-03.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems~~, ~~and~~ their associated Electronic Access Control or Monitoring Systems (EACMS), ~~and~~ Physical Access Control Systems (PACS), and the SCI hosting high or medium impact BCS or their associated Electronic Access Controlling or Monitoring System (EACMS) or Physical Access Control System (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- 1.1.** One or more process(es) used in planning for the procurement of ~~SCI, BES Cyber Systems~~BCS, and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System (BES) from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
- 1.2.** One or more process(es) used in procuring ~~SCI, BES Cyber Systems~~BCS, and their associated EACMS and PACS, that address the following, as applicable:
- 1.2.1.** Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- 1.2.2.** Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- 1.2.3.** Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
- 1.2.4.** Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;
- 1.2.5.** Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the ~~SCI, BES Cyber System~~BCS and their associated EACMS and PACS; and
- 1.2.6.** Coordination of controls for vendor-initiated remote access.
- M1.** Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.
- R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

- M2.** Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.
- R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- M3.** Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

“Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) 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 Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in Part 1.2, but the plans do not include one of the parts	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in Part 1.2, but the plans do not include two or more of the parts in <u>Requirement R1</u>	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in <u>Requirement R1</u> Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in <u>Requirement R1</u> Part 1.2.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	in <u>Requirement R1</u> Part 1.2.1 through Part 1.2.6.	Part 1.2.1 through Part 1.2.6.		OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS,~~ <u>PACS, and SCI</u> , to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring ~~BES Cyber~~	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS,~~ <u>PACS, and SCI</u> , to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring ~~BES Cyber~~	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS,~~ <u>PACS, and SCI</u> , to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS,~~ <u>PACS, and SCI</u> , to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~BES Cyber Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	~~BES Cyber Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan” ~~for Project 2019-03~~
- ~~CIP-013-2 Technical Rationale~~

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
<u>3</u>	<u>TBD</u>	<u>Virtualization conforming changes.</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2020
10-day final ballot	September 2020
Board adoption	November 2020

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-~~76~~
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.~~ 4.1.5. Reliability Coordinator

4.1.7.4.1.6. Transmission Operator**4.1.8.4.1.7. 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-~~67~~:

- 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-004-67.

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” or “Applicability” column. The “Applicable Systems” column ~~to~~ further defines 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

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-67 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-004-67 Table R1 – Security Awareness Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-67 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 • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

- 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-~~76~~ 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-~~76~~ Table R2 – *Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-67 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 <u>(BCSI)</u> 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-004-67 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.

- 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-004-67 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-004-67 Table R3 – Personnel Risk Assessment Program and additional evidence to demonstrate implementation of the program(s).

CIP-004-67 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 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 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 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.

- 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-004-67 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-004-67 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-004-67 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; <u>and</u> 4.1.2. Unescorted physical access into a Physical Security Perimeter; <u>and</u> ~~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 <u>and</u>, unescorted physical access in a Physical Security Perimeter; <u>and</u> ~~access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~

CIP-004-6 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 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 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: 0. ~~EACMS~~; and 0. ~~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: 0. ~~A dated listing of authorizations for BES Cyber System information;~~ 0. ~~Any privileges associated with the authorizations; and~~ 0. ~~Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.~~

- 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-004-67 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-004-67 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-67 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 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-Table-R5—Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	High Impact BES Cyber Systems and their associated: 0. ~~EACMS~~; and 0. ~~PACS~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 0. ~~EACMS~~; and 0. ~~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-004-67 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.43	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-004-26 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.54	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.

- R6.** Each Responsible Entity shall implement one or more documented access management program(s) for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M6.** Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicability	Requirements	Measures
6.1	<u>BCSI associated with:</u> <u>High Impact BES Cyber Systems and their associated:</u> <u>EACMS; and</u> <u>PACS</u> <u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> <u>EACMS; and</u> <u>PACS</u>	<u>Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.</u>	<u>Examples of evidence may include, but are not limited to, the following:</u> <u>Dated authorization records for provisioned access to BCSI based on need; or</u> <u>List of authorized individuals</u>

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicability	Requirements	Measures
6.2	<u>BCSI associated with:</u> <u>High Impact BES Cyber Systems and their associated:</u> <u>EACMS; and</u> <u>PACS</u> <u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> <u>EACMS; and</u> <u>PACS</u>	<u>Verify at least once every 15 calendar months that all provisioned access to BCSI:</u> <u>6.2.1. Is authorized; and</u> <u>6.2.2. Is appropriate based on need, as determined by the Responsible Entity.</u>	<u>Examples of evidence may include, but are not limited to, all of the following:</u> <u>List of authorized individuals; and</u> <u>List of individuals who have been provisioned access; and</u> <u>List of privileges associated with the authorizations; and</u> <u>List of privileges associated with the provisioned access; and</u> <u>Dated documentation of the 15-calendar-month verification; and</u> <u>Documented reconciliation actions, if any.</u>
6.3	<u>BCSI associated with:</u> <u>High Impact BES Cyber Systems and their associated:</u> <u>EACMS; and</u> <u>PACS</u> <u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> <u>EACMS; and</u> <u>PACS</u>	<u>For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.</u>	<u>Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.</u>

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

~~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.~~

~~**1.3.1.2. Evidence Retention:** The following evidence retention period(s) 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 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 Applicable~~ entity shall keep data or evidence to show compliance as identified below unless directed by its CEA-Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- ~~Each The Responsible Applicable~~ entity shall retain evidence of each requirement in this standard for three calendar years.
- If an ~~Responsible Applicable~~ 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 Compliance Enforcement Authority ~~CEA~~ shall keep the last audit records and all requested and submitted subsequent audit records.

~~**1.4.1.3. Compliance Monitoring and Assessment Processes:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot-Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.5. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-67)			
			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-004-67)			
			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-004-67)			
			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-004-67)			
			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-004-67)			
			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-004-67)			
			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-004-67)			
			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-004-67)			
			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 <u>not</u> implemented one or more documented program(s) for access management that includes a process to authorize electronic access, <u>or</u> unescorted physical access, <u>or</u> ~~access to the designated storage locations where BES Cyber System Information is located.~~ (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-67)			
			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-004-67)			
			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-004-67)			
			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 <u>or</u>, 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-004-67)			
			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. (5.43) OR The Responsible	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-004-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (5.54) OR The Responsible	~~termination action. (5.3)~~	~~date and time of the termination action. (5.3)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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 circumstances. (5.54)			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<u>R6</u>	<u>Same Day Operations and Operations Planning</u>	<u>Medium</u>	<u>The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement one of the applicable items for Parts 6.1 through 6.3. (R6)</u>	<u>The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement two of the applicable items for Parts 6.1 through 6.3. (R6)</u>	<u>The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement three of the applicable items Parts 6.1 through 6.3. (R6)</u>	<u>The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)</u>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

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.	

Version	Date	Action	Change Tracking
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
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Adopted by the NERC Board of Trustees</u>	<u>Revised to enhance BES reliability for entities to manage their BCSl.</u>

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

~~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~~

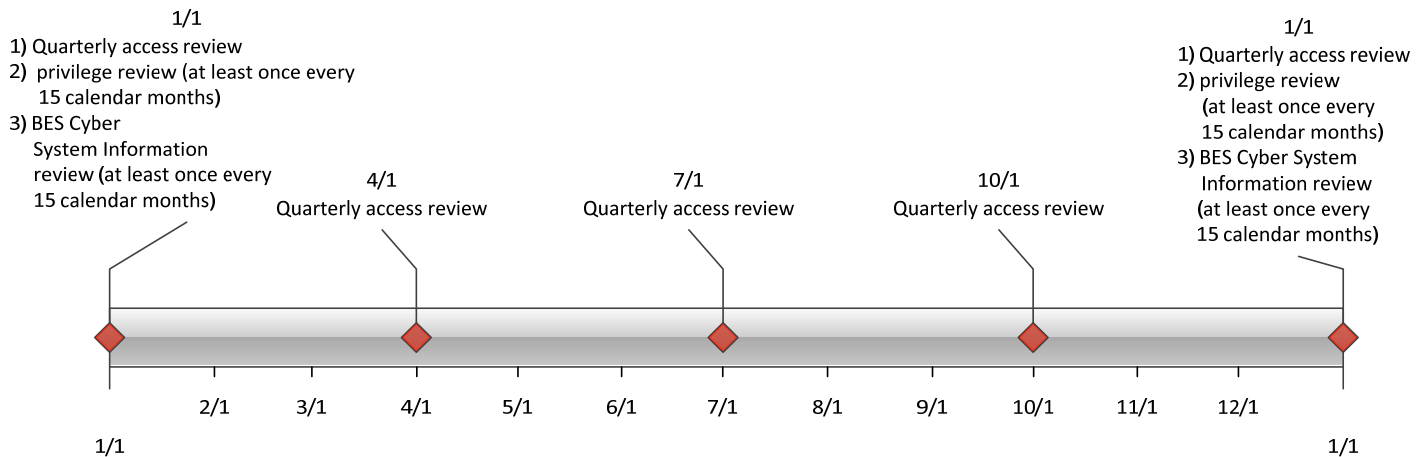
~~collective bargaining unit agreements. When it is not possible to perform a full seven-year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under 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 be 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.~~

Rationale:

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

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.~~

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.~~

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.~~

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. "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 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.~~

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).~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal or informal comment period with ballot	July 2020
10-day final ballot	September 2020
Board adoption	November 2020

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-~~23~~
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) 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~~4.1.5 Reliability Coordinator

4.1.74.1.6 Transmission Operator**4.1.84.1.7 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-~~23~~:

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-~~23~~.

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” and “Applicability” Columns in Tables:

Each table has an “Applicable Systems” or “Applicability” column. The “Applicable Systems” column ~~to~~ further defines 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

- 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-~~23~~ Table R1 – Information Protection Program. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.
- M1.** Evidence for the information protection program must include the applicable requirement parts in CIP-011-~~23~~ Table R1 – Information Protection Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-23 Table R1 – Information Protection Program

Part	Applicability Systems	Requirements	Measures
1.1	<u>BCSI pertaining to:</u> 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~~ <u>BCSI</u>.	Examples of acceptable evidence include, but are not limited to, <u>the following:</u> • Documented method(s) to identify ~~BES Cyber System Information~~ <u>BCSI</u> from <u>the</u> entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~ <u>BCSI</u> as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to ~~recognize~~ <u>identify</u> ~~BES Cyber System Information~~ <u>BCSI</u>; or • ~~Repository or electronic and physical~~ <u>Storage</u> location <u>identified</u> ~~designated~~ for housing ~~BES Cyber System Information~~ <u>BCSI</u> in the entity's information protection program.

CIP-011-23 Table R1 – Information Protection Program

Part	Applicability	Requirements	Measures
1.2	<u>BCSI as identified in Part 1.1</u> <u>High Impact BES Cyber Systems and their associated:</u> <u>1. EACMS; and</u> <u>2. PACS</u> <u>Medium Impact BES Cyber Systems and their associated:</u> <u>1. EACMS; and</u> <u>PACS</u>	<u>Procedure/Method(s) to for protecting and protect and securely handling BES Cyber System Information BCSI, including storage, transit, and use.</u>	Examples of acceptable evidence include, but are not limited to, <u>the following:</u> • <u>Evidence of methods used to protect and securely handle BCSI during its lifecycle, including:</u> <u>o Electronic mechanisms,</u> <u>o Physical mechanisms,</u> <u>o Technical mechanisms, or</u> <u>o Administrative mechanisms.</u> <u>Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or</u> • <u>Records indicating that BES Cyber System Information BCSI is handled in a manner consistent with the entity's documented procedure(s).</u>

CIP-011-3 Table R1 – Information Protection Program			
<u>Part</u>	<u>Applicability</u>	<u>Requirement</u>	<u>Measure</u>

1.3	<u>BCSI as identified in Part 1.1</u>	<u>When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s) for the following:</u> <u>1.3.1 Data governance and rights management; and</u> <u>1.3.2 Identity and access management; and</u> <u>1.3.3 Security management; and</u> <u>1.3.4 Application, infrastructure, and network security.</u>	<u>Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:</u> • <u>Implementation of the risk identification and assessment method(s) (1.3);</u> • <u>List of risk identification and assessment method(s) per vendor (1.3.1);</u> • <u>Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4);</u> • <u>Business agreements that include communication expectations and protocols for disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1);</u> • <u>Consideration made for data sovereignty, if any (1.3.1);</u>

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure
			• <u>Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3);</u> • <u>Dated documentation of vendor’s identity and access management program(1.3.2); and</u> • <u>Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).</u>

CIP-011-3 Table R1 — Information Protection Program

Part	Applicability	Requirement	Measure
1.4	<u>BCSI as identified in Part 1.1</u>	<u>When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.</u>	<u>Examples of evidence may include, but are not limited to, dated documentation of the following:</u> <u>• Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]);</u> <u>• Evidence of implementation (e.g., configuration files, command output, architecture documents); and</u> <u>• Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.</u>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-~~23~~ 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-~~23~~ 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- ~~23~~ 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~~<u>BCSI</u> (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~~<u>BCSI</u> 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~~<u>BCSI</u> 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~~<u>BCSI</u>.

CIP-011-~~23~~ 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 <u>BCSIBES</u> ~~Cyber System Information~~, the Responsible Entity shall take action to prevent the unauthorized retrieval of <u>BCSIBES</u> ~~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 <u>BCSIBES</u> ~~Cyber Information~~ prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

~~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.~~

~~**1.3.1.2. Evidence Retention:** The following evidence retention period(s) 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 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-applicable E~~entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority~~CEA~~ to retain specific evidence for a longer period of time as part of an investigation:

- ~~Each-The Responsible-applicable E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If a ~~n Responsible-applicable E~~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 Compliance Enforcement Authority~~CEA~~ shall keep the last audit records and all requested and submitted subsequent audit records.

1.4.1.3. Compliance Monitoring and Assessment Processes: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~

• ~~Self-Reporting~~

• ~~Complaints~~

~~1.5. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- ~~23~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	~~N/A~~ <u>The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the applicable items for Parts 1.1 through 1.4. (R1)</u>	~~N/A~~ <u>The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the applicable items for Parts 1.1 through 1.4. (R1)</u>	~~N/A~~ <u>The Responsible Entity implemented one or more documented information protection program(s) but did not implement three or more of the applicable items for Parts 1.1 through 1.4. (R1)</u>	The Responsible Entity ~~has~~ <u>did</u> not ~~documented or~~ implemented <u>one or more a documented BES Cyber System</u> information protection program(s). (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~~ <u>BCSI</u> from	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~~ <u>BCSI</u> from	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011- ~~23~~ Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- ~~23~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the BES Cyber Asset. (2.1)	the BES Cyber Asset. (2.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents~~Guideline and Technical Basis (attached).~~**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.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	

<u>3</u>	<u>TBD</u>	<u>Adopted by the NERC Board of Trustees</u>	<u>Revised to enhance BES reliability for entities to manage their BCSl.</u>

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

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 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.~~

Rationale:

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

Rationale for Requirement R1:

~~The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

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.~~

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information

SAR Title:	PRC-005-6 applicability to AVR protective functions		
Date Submitted:	6/8/2020		
SAR Requester			
Name:	Brian Kasmarzik, Chair		
Organization:	Project 2019-04 Modifications to PRC-005-6 SAR Drafting Team		
Telephone:	314-554-4315	Email:	BKasmarzik@ameren.com

SAR Type (Check as many as apply)

☒ ☒ ☒ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ ☐ Revision to Existing Standard	☐ Variance development or revision
☒ ☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

PRC-005-~~6~~ will be revised to provide clarity that the BES protective functions enabled within excitation systems (including analog/digital Automatic Voltage Regulators (AVRs)), and BES protective functions enabled within other control systems, that respond to electrical quantities ~~and act to cease injecting current (75 MVA or greater) or and~~ trip BES elements either directly or via lockout or auxiliary tripping relays are within the scope of the standard. The clarity that is needed is regarding protective functions inside excitation systems and control systems which are not stand-alone relays, but otherwise perform as a BES Protection System. Without clear applicability, the industry is struggling with how to implement PRC-005 and what testing is acceptable to meet the required maintenance activities prescribed by PRC-005. The lack of clarity presents a reliability gap in the application of PRC-005.

Additionally, there are Protection System ~~Station-station~~ direct current (DC) supply technologies that do not currently have maintenance activities established in PRC-005. The standard needs to address battery-based station DC technologies that are not covered by PRC-005 and consider other emerging alternative technologies, both battery-based and non-battery-based.

Requested information
This project would modify Reliability Standard PRC-005-~~6~~ to be consistent with the Federal Energy Regulatory Commission (FERC)-approved changes to registration as part of the Risk Based Registration (RBR) initiative by specifying Underfrequency Load Shedding (UFLS)-only Distribution Providers (DPs) in the Applicability Section.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
Provide clear, unambiguous applicability of PRC-005 to protective functions and provide the specificity needed for the industry to consistently identify and implement the required maintenance activities.
Provide for the use of <u>emerging alternative</u> Protection System <u>Station-station</u> DC supply technologies, battery based and non-battery-based, and ensure that they are subject to maintenance requirements.
This project would modify Reliability Standard PRC-005-~~6~~ to be consistent with the FERC-approved changes to registration as part of the RBR initiative and to add UFLS-only DPs in the Applicability Section.
Project Scope (Define the parameters of the proposed project):
Modify PRC-005 to provide clarity that the <u>BES</u> protective functions enabled within analog/digital AVRs, excitation systems, and <u>BES protective functions enabled within</u> other control systems that respond to electrical quantities ~~and act to cease injecting current and~~ trip BES elements either directly or via lockout or auxiliary tripping relays are within the scope of the standard. Modifications to PRC-005-~~6~~ could also include defining terms, revising applicability, modifying maintenance activities and intervals, or other appropriate modifications needed to provide clarity. In addition, modify the PRC-005-~~6~~ Supplementary Reference and FAQ to align with revisions to PRC-005-~~6~~.
The clarifying changes would apply to BES Protection Systems and <u>BES</u> protective functions applied on generators, dispersed power-producing resources from the point of aggregation (greater than 75 MVA) to the point of Interconnection, static and synchronous condensers and other BES elements as defined.
Modify PRC-005-~~6~~ to establish maintenance requirements for Protection System DC supply technologies that are not currently covered.
This project would modify Reliability Standard PRC-005-~~6~~ to be consistent with the FERC-approved changes to registration as part of the RBR initiative and to add UFLS-only DPs in the Applicability Section.

Requested information

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):

The North American Generator Forum (NAGF) received feedback from members indicating that there was confusion regarding the applicability of protective functions inside synchronous generator excitation systems to PRC-005. The primary cause of confusion is the use of the NERC term "Protection System," which specifies "relays" but not the protective functions that are typically (but not always) associated with relays. Excitation systems may measure and utilize similar quantities as protective relays and may perform similar functions as protective relays applicable to PRC-005. For this reason, the SAR drafting team agrees that the aforementioned protective functions within excitation systems and other control systems need to be clearly and explicitly applicable to PRC-005.

PRC-005 will be modified to provide clarity on the inclusion of BES protective functions enabled within excitation systems (analog/digital AVR), and BES protective functions enabled within other control systems, that respond to electrical quantities and ~~act to cease injecting current~~ or trip BES elements either directly or via lockout or auxiliary tripping relays. The clarifying changes would apply to BES Protection Systems and BES protective functions applied on generators, dispersed power producing resources from the point of aggregation (greater than 75 MVA) to the point of Interconnection, static and synchronous condensers and other BES elements as defined.

The SAR drafting team recommends considering the specification of American National Standards Institute (ANSI) Standard Device Numbers for the applicability to PRC-005 as outlined in the Applicability Section 4.2. Other options to provide clarity include: developing standard-specific definitions, developing or revising existing terms in the NERC Glossary of Terms, or making other modifications to the Applicability section.

The maintenance tables should be updated to include the aforementioned BES protective functions enabled within other control systems, and the associated maintenance activities and intervals. -

Additionally, the maintenance tables should be updated to include new DC supply technologies for Protection System(s) not currently captured.

Entities registered as ULFS-Only (DPs) have PRC-005-~~6~~ applicable Protection Systems, but are not expressly listed as Applicable Entities in Section 4.1 UFLS-Only DPs should be added to the Applicability Section to avoid any confusion and to be consistent with the FERC-approved RBR registration changes.

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information	
The SAR DT is seeking industry input regarding cost impact.	
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):	
The clarifying changes would apply to BES Protection Systems and BES protective functions applied on generators, dispersed power producing resources from the point of aggregation (greater than 75 MVA) to the point of Interconnection, static and synchronous condensers and other BES elements as defined. The items under consideration related to DC supply technologies would impact multiple facility owners.	
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):	
Generator Owner (GO), Transmission Owner (TO), Distribution Provider (DP), Underfrequency Load Shedding (UFLS)-only DP	
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.	
The NAGF and the NEI worked together to generate the initial SAR and communicated the issue in advance to NERC.	
This project would modify Reliability Standard PRC-005- ~~6~~ to be consistent with the FERC-approved changes to registration as part of the RBR initiative and to add UFLS-only DPs in the Applicability Section.	
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?	
Options to provide clarity for PRC-005 include: developing standard-specific definitions, developing or revising existing terms in the NERC Glossary of Terms, or making other modifications to the Applicability section. In the event of developing or revising existing terms in the NERC Glossary of Terms, review of the effects on other standards must be performed.	
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.	

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those 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.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
☐	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.

Market Interface Principles	
Does the proposed standard development project 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
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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
<i>e.g.</i> , NPCC	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

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.

Description of Current Draft

This is the first draft of the proposed standard for a formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title:** Emergency ~~Preparedness Operations~~
2. **Number:** EOP-011-~~21~~
3. **Purpose:** To ~~effects of operating Emergencies by~~ ensuring each Transmission Operator, ~~and~~ Balancing Authority, ~~and~~ Generator Owner has developed ~~Operating P~~lan(s) to mitigate ~~and prepare for~~ operating Emergencies; ~~and that those Operating pPlans~~ are coordinated within a Reliability Coordinator Area.
4. **Applicability:**
 - 4.1. **Functional Entities:**
 - 4.1.1 Balancing Authority
 - 4.1.2 Reliability Coordinator
 - ~~4.1.3~~ Transmission Operator
 - ~~4.1.4~~ Generator Owner
 - 4.2. **Facilities**
 - ~~4.2.1~~ For the purpose of this standard, the term “generating unit” includes all BES generating units and BES generating plants.
5. **Effective Date:** See Implementation Plan for ~~EOP-011-1~~ Project 2019-06.
- ~~6. Background:~~

~~EOP-011-1 consolidates requirements from three standards: EOP-001-2.1b, EOP-002-3.1, and EOP-003-2.~~

~~The standard streamlines the requirements for Emergency operations for the Bulk Electric System into a clear and concise standard that is organized by Functional Entity. In addition, the revisions clarify the critical requirements for Emergency Operations, while ensuring strong communication and coordination across the Functional Entities.~~

B. Requirements and Measures

- R1. Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*
 - 1.1. Roles and responsibilities for activating the Operating Plan(s);
 - 1.2. Processes to prepare for and mitigate Emergencies including:
 - 1.2.1. Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;
 - 1.2.2. Cancellation or recall of Transmission and generation outages;

- 1.2.3. Transmission system reconfiguration;
- 1.2.4. Redispatch of generation request;
- 1.2.5. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and
- 1.2.6. Reliability impacts of:
 - 1.2.6.1. cold weather conditions; and
 - ~~1.2.5.1.~~1.2.6.2. any other extreme weather conditions.

M1. Each Transmission Operator will have a dated Operating Plan(s) developed in accordance with Requirement R1 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R1.

R2. Each Balancing Authority shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate Capacity Emergencies and Energy Emergencies within its Balancing Authority Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

- 2.1. Roles and responsibilities for activating the Operating Plan(s);
- 2.2. Processes to prepare for and mitigate Emergencies including:
 - 2.2.1. Notification to its Reliability Coordinator, to include current and projected conditions when experiencing a Capacity Emergency or Energy Emergency;
 - 2.2.2. Requesting an Energy Emergency Alert, per Attachment 1;
 - 2.2.3. Managing generating resources in its Balancing Authority Area to address:
 - 2.2.3.1. capability and availability;
 - 2.2.3.2. fuel supply and inventory concerns;
 - 2.2.3.3. fuel switching capabilities; and
 - 2.2.3.4. environmental constraints.
 - 2.2.4. Public appeals for voluntary Load reductions;
 - 2.2.5. Requests to government agencies to implement their programs to achieve necessary energy reductions;
 - 2.2.6. Reduction of internal utility energy use;

- 2.2.7. Use of Interruptible Load, curtailable Load and demand response;
- 2.2.8. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

2.2.9. Reliability impacts of:

2.2.9.1. cold weather conditions; and

~~2.2.8.1.2.2.9.2.~~ any other extreme weather conditions.

- M2.** Each Balancing Authority will have a dated Operating Plan(s) developed in accordance with Requirement R2 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R2.
- R3.** The Reliability Coordinator shall review the Operating Plan(s) to mitigate operating Emergencies submitted by a Transmission Operator or a Balancing Authority regarding any reliability risks that are identified between Operating Plans. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*
 - 3.1.** Within 30 calendar days of receipt, the Reliability Coordinator shall:
 - 3.1.1.** Review each submitted Operating Plan(s) on the basis of compatibility and inter-dependency with other Balancing Authorities' and Transmission Operators' Operating Plans;
 - 3.1.2.** Review each submitted Operating Plan(s) for coordination to avoid risk to Wide Area reliability; and
 - 3.1.3.** Notify each Balancing Authority and Transmission Operator of the results of its review, specifying any time frame for resubmittal of its Operating Plan(s) if revisions are identified.
- M3.** The Reliability Coordinator will have documentation, such as dated e-mails or other correspondences that it reviewed Transmission Operator and Balancing Authority Operating Plans within 30 calendar days of submittal in accordance with Requirement R3.
- R4.** Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator. *[Violation Risk Factor: High] [Time Horizon: Operation Planning]*
- M4.** The Transmission Operator and Balancing Authority will have documentation, such as dated emails or other correspondence, with an Operating Plan(s) version history showing that it responded and updated the Operating Plan(s) within the timeframe identified by its Reliability Coordinator in accordance with Requirement R4.

- R5.** Each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority within its Reliability Coordinator Area shall notify, within 30 minutes from the time of receiving notification, other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*
- M5.** Each Reliability Coordinator that receives an Emergency notification from a Balancing Authority or Transmission Operator within its Reliability Coordinator Area will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that will be used to determine if the Reliability Coordinator communicated, in accordance with Requirement R5, with other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators .
- R6.** Each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall declare an Energy Emergency Alert, as detailed in Attachment 1. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*
- M6.** Each Reliability Coordinator, with a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area, will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that it declared an Energy Emergency Alert, as detailed in Attachment 1, in accordance with Requirement R6.
- R7. Each Generator Owner shall develop, maintain, and implement one or more cold weather preparedness plan(s) for its generating unit(s). The cold weather preparedness plan(s) shall include the following, at a minimum: [Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-Time Operations]**
- 7.1. Generating unit(s) freeze protection measures based on unique factors such as geographical location and plant configuration;**
- 7.2. Annual maintenance and inspection of generating unit(s) freeze protection measures; and**
- 7.3. Generating unit(s) cold weather data, to include:**
- 7.3.1. Generating unit(s) operating limitations in cold weather; and**
- 7.3.2. Generating unit(s):**
- 7.3.2.1. minimum design temperature; or**
- 7.3.2.2. minimum demonstrated historical performance during cold weather in the previous 5 years;**
- 7.4. Awareness training on the roles and responsibilities of site personnel contained in the cold weather preparedness plan.**

M7. Each Generator Owner shall have a documented cold weather preparedness plan in accordance with Requirement R7; and have evidence such as (a review or revision history to indicate that the plan has been maintained;) and have evidence such as operator checklists, work orders, test records, other operating and maintenance documentation, or other communication documentation to show that its cold weather preparedness plan was implemented; and have evidence such as training materials and attendance list showing successful completion of training.

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, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with the mandatory and enforceable NERC Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

~~The Balancing Authority, Reliability Coordinator, and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation. 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 following evidence retention period(s) 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 applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Transmission Operator shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R1 and R4 and Measures M1 and M4.
- The Balancing Authority shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R2 and R4, and Measures M2 and M4.
- The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.
- The Generator Owner shall retain the cold weather preparedness plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirement R7 and Measure M7.

~~If a Balancing Authority, Reliability Coordinator or Transmission Operator is found non-compliant, it shall keep information related to the non-compliance until found compliant.~~

~~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~~Enforcement Program:

As defined in the NERC Rules of Procedure; “Compliance Monitoring and ~~Assessment~~Enforcement Processes~~Program~~” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated ~~R~~Reliability ~~s~~Standard.

~~1.4. Additional Compliance Information~~

~~None~~

Table of Compliance Elements

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to maintain it.	The Transmission Operator developed an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to have it reviewed by its Reliability Coordinator.	The Transmission Operator failed to develop an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. OR The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to implement it.
R2	Real-time Operations, Operations	High	N/A	The Balancing Authority developed a Reliability	The Balancing Authority developed an Operating Plan(s)	The Balancing Authority failed to develop an

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning, Long-term Planning			Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to maintain it.	to mitigate operating Emergencies within its Balancing Authority Area but failed to have it reviewed by its Reliability Coordinator.	Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area. OR The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to implement it.
R3	Operations Planning	High	N/A	N/A	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Operator within 30 calendar days.	
R4	Operations Planning	High	N/A	N/A	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator within the timeframe specified by its Reliability Coordinator.	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator.
R5	Real-time Operations	High	N/A	N/A	The Reliability Coordinator that received an Emergency notification from a Transmission Operator or Balancing Authority did not notify neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators but failed	The Reliability Coordinator that received an Emergency notification from a Transmission Operator or Balancing Authority failed to notify neighboring Reliability Coordinators, Balancing Authorities and

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to notify within 30 minutes from the time of receiving notification.	Transmission Operators.
R6	Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator that had a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area failed to declare an Energy Emergency Alert.
<u>R7</u>	<u>Operations Planning and Real-time Operations</u>	<u>High</u>	<u>The Generator Owner's cold weather preparedness plan failed to include one of the applicable requirement Parts within Requirement R7.</u>	<u>The Generator Owner developed a cold weather preparedness plan(s) but failed to maintain it.</u> <u>OR</u> <u>The Generator Owner's cold weather preparedness plan failed to include two</u>	<u>The Generator Owner developed and maintained a cold weather preparedness plan(s) but failed to fully implement it.</u> <u>OR</u> <u>The Generator Owner's cold weather preparedness plan</u>	<u>The Generator Owner does not have a cold weather preparedness plan.</u> <u>OR</u> <u>The Generator Owner has a cold weather</u>

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>of the applicable requirement Parts within Requirement R7.</u>	<u>failed to include three of the applicable requirement Parts within Requirement R7.</u>	<u>preparedness plan, but failed to include all the applicable requirement Parts within Requirement R7.</u>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by Board of Trustees	Merged EOP-001-2.1b, EOP-002-3.1 and EOP-003-2.
1	November 19, 2015	FERC approved EOP-011-1. Docket Nos. RM15-7-000, RM15-12-000, and RM15-13-000. Order No. 818	
<u>2</u>	<u>TBD</u>	<u>Adopted by the Board of Trustees</u>	<u>Revised under Project 2019-06</u>

Attachment 1-EOP-011-~~21~~
Energy Emergency Alerts

Introduction

This Attachment provides the process and descriptions of the levels used by the Reliability Coordinator in which it communicates the condition of a Balancing Authority which is experiencing an Energy Emergency.

A. General Responsibilities

- 1. Initiation by Reliability Coordinator.** An Energy Emergency Alert (EEA) may be initiated only by a Reliability Coordinator at 1) the Reliability Coordinator's own request, or 2) upon the request of an energy deficient Balancing Authority.
- 2. Notification.** A Reliability Coordinator who declares an EEA shall notify all Balancing Authorities and Transmission Operators in its Reliability Coordinator Area. The Reliability Coordinator shall also notify all neighboring Reliability Coordinators.

B. EEA Levels

Introduction

To ensure that all Reliability Coordinators clearly understand potential and actual Energy Emergencies in the Interconnection, NERC has established three levels of EEAs. The Reliability Coordinators will use these terms when communicating Energy Emergencies to each other. An EEA is an Emergency procedure, not a daily operating practice, and is not intended as an alternative to compliance with NERC Reliability Standards.

The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially.

1. EEA 1 — All available generation resources in use.

Circumstances:

- The Balancing Authority is experiencing conditions where all available generation resources are committed to meet firm Load, firm transactions, and reserve commitments, and is concerned about sustaining its required Contingency Reserves.
- Non-firm wholesale energy sales (other than those that are recallable to meet reserve requirements) have been curtailed.

2. EEA 2 — Load management procedures in effect.

Circumstances:

- The Balancing Authority is no longer able to provide its expected energy requirements and is an energy deficient Balancing Authority.
- An energy deficient Balancing Authority has implemented its Operating Plan(s) to mitigate Emergencies.

- An energy deficient Balancing Authority is still able to maintain minimum Contingency Reserve requirements.

During EEA 2, Reliability Coordinators and energy deficient Balancing Authorities have the following responsibilities:

2.1 Notifying other Balancing Authorities and market participants. The energy deficient Balancing Authority shall communicate its needs to other Balancing Authorities and market participants. Upon request from the energy deficient Balancing Authority, the respective Reliability Coordinator shall post the declaration of the alert level, along with the name of the energy deficient Balancing Authority on the RCIS website.

2.2 Declaration period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 2 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators.

2.3 Sharing information on resource availability. Other Reliability Coordinators of Balancing Authorities with available resources shall coordinate, as appropriate, with the Reliability Coordinator that has an energy deficient Balancing Authority.

2.4 Evaluating and mitigating Transmission limitations. The Reliability Coordinator shall review Transmission outages and work with the Transmission Operator(s) to see if it's possible to return to service any Transmission Elements that may relieve the loading on System Operating Limits (SOLs) or Interconnection Reliability Operating Limits (IROLs).

2.5 Requesting Balancing Authority actions. Before requesting an EEA 3, the energy deficient Balancing Authority must make use of all available resources; this includes, but is not limited to:

2.5.1 All available generation units are on line. All generation capable of being on line in the time frame of the Emergency is on line.

2.5.2 Demand-Side Management. Activate Demand-Side Management within provisions of any applicable agreements.

3. EEA 3 —Firm Load interruption is imminent or in progress.

Circumstances:

- The energy deficient Balancing Authority is unable to meet minimum Contingency Reserve requirements.

During EEA 3, Reliability Coordinators and Balancing Authorities have the following responsibilities:

3.1 Continue actions from EEA 2. The Reliability Coordinators and the energy deficient Balancing Authority shall continue to take all actions initiated during EEA 2.

3.2 Declaration Period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 3 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities, and Transmission Operators.

3.3 Reevaluating and revising SOLs and IROLs. The Reliability Coordinator shall evaluate the risks of revising SOLs and IROLs for the possibility of delivery of energy to the energy deficient Balancing Authority. Reevaluation of SOLs and IROLs shall be coordinated with other Reliability Coordinators and only with the agreement of the Transmission Operator whose Transmission Owner (TO) equipment would be affected. SOLs and IROLs shall only be revised as long as an EEA 3 condition exists, or as allowed by the Transmission Owner whose equipment is at risk. The following are minimum requirements that must be met before SOLs or IROLs are revised:

3.3.1 Energy deficient Balancing Authority obligations. The energy deficient Balancing Authority, upon notification from its Reliability Coordinator of the situation, it will immediately take whatever actions are necessary to mitigate any undue risk to the Interconnection. These actions may include Load shedding.

3.4 Returning to pre-Emergency conditions. Whenever energy is made available to an energy deficient Balancing Authority such that the Systems can be returned to its pre-Emergency SOLs or IROLs condition, the energy deficient Balancing Authority shall request the Reliability Coordinator to downgrade the alert level.

3.4.1 Notification of other parties. Upon notification from the energy deficient Balancing Authority that an alert has been downgraded, the Reliability Coordinator shall notify the neighboring Reliability Coordinators (via the RCIS), Balancing Authorities and Transmission Operators that its Systems can be returned to its normal limits.

Alert 0 - Termination. When the energy deficient Balancing Authority is able to meet its Load and Operating Reserve requirements, it shall request its Reliability Coordinator to terminate the EEA.

0.1 Notification. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS of the termination. The Reliability Coordinator shall also notify the neighboring Balancing Authorities and Transmission Operators.

Guidelines and Technical Basis

Rationale:

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

Rationale for R1:

The EOP SDT examined the recommendation of the EOP Five-Year Review Team (FYRT) and FERC directive to provide guidance on applicable entity responsibility that was included in EOP-001-2.1b. The EOP SDT removed EOP-001-2.1b, Attachment 1, and incorporated it into this standard under the applicable requirements. This also establishes a separate requirement for the Transmission Operator to create an Operating Plan(s) for mitigating operating Emergencies in its Transmission Operator Area.

The Operating Plan(s) can be one plan, or it can be multiple plans.

“Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency” was retained. This is a process in the plan(s) that determines when the Transmission Operator must notify its Reliability Coordinator.

To meet the associated measure, an entity would likely provide evidence that such an evaluation was conducted along with an explanation of why any overlap of Loads between manual and automatic load shedding was unavoidable or reasonable.

An Operating Plan(s) is implemented by carrying out its stated actions.

If any Parts of Requirement R1 are not applicable, the Transmission Operator should note “not applicable” in the Operating Plan(s). The EOP SDT recognizes that across the regions, Operating Plan(s) may not include all the elements listed in this requirement due to restrictions, other methods of managing situations, and documents that may already exist that speak to a process that already exists. Therefore, the entity must provide in the plan(s) that the element is not applicable and detail why it is not applicable for the plan(s).

With respect to automatic Load shedding schemes that include both UVLS and UFLS, the EOP SDT’s intent is to keep manual and automatic Load shed schemes as separate as possible, but realizes that sometimes, due to system design, there will be overlap. The intent in Requirement R1 Part 1.2.5, is to minimize, as much as possible, the use of manual Load shedding which is already armed for automatic Load shedding. The automatic Load shedding schemes are the important backstops against Cascading outages or System collapse. If any entity manually sheds a Load which was included in an automatic scheme, it reduces the effectiveness of that automatic scheme. Each entity should review their automatic Load shedding schemes and coordinate their manual processes so that any overlapping use of Loads is avoided to the extent reasonably possible.

Rationale for R2:

~~To address the recommendation of the FYRT and the FERC directive to provide guidance on applicable entity responsibility in EOP-001-2.1b, Attachment 1, the EOP SDT removed EOP-001-2.1b, Attachment 1, and incorporated it into this standard under the applicable requirements. EOP-011-1 also establishes a separate requirement for the Balancing Authority to create its Operating Plan(s) to address Capacity and Energy Emergencies.~~

~~The Operating Plan(s) can be one plan, or it can be multiple plans.~~

~~An Operating Plan(s) is implemented by carrying out its stated actions.~~

~~If any Parts of Requirement R2 are not applicable, the Balancing Authority should note “not applicable” in the Operating Plan(s). The EOP SDT recognizes that across the regions, Operating Plan(s) may not include all the elements listed in this requirement due to restrictions, other methods of managing situations, and documents that may already exist that speak to a process that already exists. Therefore, the entity must provide in the plan(s) that the element is not applicable and detail why it is not applicable for the plan(s).~~

~~The EOP SDT retained the statement “Operator controlled manual Load shedding,” as it was in the current EOP-003-2 and is consistent with the intent of the EOP SDT.~~

~~With respect to automatic Load shedding schemes that include both UVLS and UFLS, the EOP SDT’s intent is to keep manual and automatic Load shedding schemes as separate as possible, but realizes that sometimes, due to system design, there will be overlap. The intent in Requirement R2 Part 2.2.8. is to minimize as much as possible the use manual Load shedding which is already armed for automatic Load shedding. The automatic Load shedding schemes are the important backstops against Cascading outages or System collapse. If an entity manually sheds a Load that was included in an automatic scheme, it reduces the effectiveness of that automatic scheme. Each entity should review its automatic Load shedding schemes and coordinate its manual processes so that any overlapping use of Loads is avoided to the extent possible.~~

~~The EOP SDT retained Requirement R8 from EOP-002-3.1 and added it to the Parts in Requirement R2.~~

Rationale for R3:

~~The SDT agreed with industry comments that the Reliability Coordinator does not need to approve BA and TOP plan(s). The SDT has changed this requirement to remove the approval but still require the RC to review each entity’s plan(s), looking specifically for reliability risks. This is consistent with the Reliability Coordinator’s role within the Functional Model and meets the FERC directive regarding the RC’s involvement in Operating Plan(s) for mitigating Emergencies.~~

Rationale for Requirement R4:

~~Requirement R4 supports the coordination of Operating Plans within a Reliability Coordinator Area in order to identify and correct any Wide Area reliability risks. The EOP SDT expects the Reliability Coordinator to make a reasonable request for response time. The time period~~

~~requested by the Reliability Coordinator to the Transmission Operator and Balancing Authority to update the Operating Plan(s) will depend on the scope and urgency of the requested change.~~

Rationale for R5

~~The EOP SDT used the existing requirement in EOP-002-3.1 for the Balancing Authority and added the words “within 30 minutes from the time of receiving notification” to the requirement to communicate the intent that timeliness is important, while balancing the concern that in an Emergency there may be a need to alleviate excessive notifications on Balancing Authorities and Transmission Operators. By adding this time limitation, a measurable standard is set for when the Reliability Coordinator must complete these notifications.~~

Rationale for Introduction

~~LSEs were removed from Attachment 1, as an LSE has no Real-time reliability functionality with respect to EEAs.~~

~~EOP-002-3.1 Requirement R9 was in place to allow for a Transmission Service Provider to change the priority of a service request, as permitted in its transmission tariff, informing the Reliability Coordinator so that the service would not be curtailed by a TLR; and since the Tagging Specs did not allow profiles to be changed, this was the only method to accomplish it. Under NAESB WEQ E-tag Specification v1811 R3.6.1.3, this has been modified and now the TSP has the ability to change the Transmission priority which, in turn, is reflected in the IDC. This technology change allows for the deletion of Requirement R9 in its entirety. Requirement R9 meets with Criterion A of Paragraph 81 and should be retired.~~

Rationale for (2) Notification

~~The EOP SDT deleted the language, “The Reliability Coordinator shall also notify all other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS). Additionally, conference calls between RCs shall be held as necessary to communicate system conditions. The RC shall also notify the other RCs when the alert has ended” as duplicative to proposed IRO-014-3 Requirement R1:~~

~~R1. Each Reliability Coordinator shall have and implement Operating Procedures, Operating Processes, or Operating Plans, for activities that require notification or coordination of actions that may impact adjacent Reliability Coordinator Areas, to support Interconnection reliability. These Operating Procedures, Operating Processes, or Operating Plans shall include, but are not limited to, the following: Communications and notifications, and the process to follow in making those notifications. Energy and capacity shortages.~~

~~Control of voltage, including the coordination of reactive resources.~~

~~Exchange of information including planned and unplanned outage information to support its Operational Planning Analyses and Real-time Assessments.~~

~~Authority to act to prevent and mitigate system conditions which could adversely impact other Reliability Coordinator Areas.~~

~~Provisions for weekly conference calls.~~

Rationale for EEA 2:

~~The EOP SDT modified the “Circumstances” for EEA 2 to show that an entity will be in this level when it has implemented its Operating Plan(s) to mitigate Emergencies but is still able to maintain Contingency Reserves.~~

Rationale for EEA 3:

~~This rationale was added at the request of stakeholders asking for justification for moving a lack of Contingency Reserves into the EEA3 category.~~

~~The previous language in EOP-002-3.1, EEA 2 used “Operating Reserve,” which is an all-inclusive term, including all reserves (including Contingency Reserves). Many Operating Reserves are used continuously, every hour of every day. Total Operating Reserve requirements are kind of nebulous since they do not have a specific hard minimum value. Contingency Reserves are used far less frequently. Because of the confusion over this issue, evidenced by the comments received, the drafting team thought that using minimum Contingency Reserve in the language would eliminate some of the confusion. This is a different approach but the drafting team believes this is a good approach and was supported by several commenters.~~

~~Using Contingency Reserves (which is a subset of Operating Reserves) puts a BA closer to the operating edge. The drafting team felt that the point where a BA can no longer maintain this important Contingency Reserves margin is a most serious condition and puts the BA into a position where they are very close to shedding Load (“imminent or in progress”). The drafting team felt that this warrants categorization at the highest level of EEA.~~

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.

Description of Current Draft

This is the first draft of proposed standard for formal a 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR) for posting	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020

Anticipated Actions	Date
45-day initial formal comment period with ballot	January 2021
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title:** Reliability Coordinator Data Specification and Collection
2. **Number:** IRO-010-~~43~~
3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring the Reliability Coordinator has the data it needs to monitor and assess the operation of its Reliability Coordinator Area.
4. **Applicability**
 - 4.1. Reliability Coordinator.
 - 4.2. Balancing Authority.
 - 4.3. Generator Owner.
 - 4.4. Generator Operator.
 - 4.5. Transmission Operator.
 - 4.6. Transmission Owner.
 - 4.7. Distribution Provider.
5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements

- R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to: *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*
 - 1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.
 - 1.2. Provisions for notification of current Protection System and ~~Special Protection System~~ Remedial Action Scheme (RAS) status or degradation that impacts System reliability.
 - 1.3. Provisions for notification of BES generating unit-specific design specification or minimum historical performance during cold weather, and expected BES generating unit operation limitations during local forecasted cold weather.
 - ~~1.2.1.4.~~ A periodicity for providing data.
 - ~~1.3.1.5.~~ The deadline by which the respondent is to provide the indicated data.
- M1. The Reliability Coordinator shall make available its dated, current, in force documented specification for data.

- R2.** The Reliability Coordinator shall distribute its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. (*Violation Risk Factor: Low*) (*Time Horizon: Operations Planning*)
- M2.** The Reliability Coordinator shall make available evidence that it has distributed its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. This evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.
- R3.** Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall satisfy the obligations of the documented specifications using: (*Violation Risk Factor: Medium*) (*Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations*)
- 3.1** A mutually agreeable format
 - 3.2** A mutually agreeable process for resolving data conflicts
 - 3.3** A mutually agreeable security protocol
- M3.** The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall make available evidence that it satisfied the obligations of the documented specification using the specified criteria. Such evidence could include but is not limited to electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority”
~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority”~~
 (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an
Applicable Governmental Authority, in their respective roles of monitoring and or
 enforcing compliance with the mandatory and enforceable ~~NERC~~-Reliability Standards
in their respective jurisdictions.

1.2. Data Evidence Retention: The following evidence retention period(s) 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 Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Reliability Coordinator shall retain its dated, current, in force documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.

The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its data specification to entities that have data required by the Reliability Coordinator’s Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.

Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

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

1.2.1.3. Compliance Monitoring and ~~Assessment Processes~~ Enforcement Program:
 As defined in the NERC Rules of Procedure, “Compliance Monitoring and ~~Assessment Processes~~
Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.3.1.4. Additional Compliance Information: None.

Table of Compliance Elements

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include <u>two or fewer</u> ~~one~~ of the parts (Part 1.1 through Part 1.54) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include <u>three</u> ~~two~~ of the parts (Part 1.1 through Part 1.54) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include <u>four</u> ~~three~~ of the parts (Part 1.1 through Part 1.54) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.54) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
						monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and Real-time	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
				Assessments.	Real-time Assessments.	Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow one of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow two of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow any of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

None

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO-010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
<u>3</u>	<u>October 30, 2020</u>	<u>FERC approved IRO-010-2. Docket No. RD20-4-000</u>	
<u>4</u>	<u>TBD</u>	<u>Adopted by NERC Board of Trustees</u>	<u>Revisions under Project 2019-06</u>

Guidelines and Technical Basis

~~Rationale:~~

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

~~Rationale for Definitions:~~

~~Changes made to the proposed definitions were made in order to respond to issues raised in NOPR paragraphs 55, 73, and 74 dealing with analysis of SOLs in all time horizons, questions on Protection Systems and Special Protection Systems in NOPR paragraph 78, and recommendations on phase angles from the SW Outage Report (recommendation 27). The intent of such changes is to ensure that Real time Assessments contain sufficient details to result in an appropriate level of situational awareness. Some examples include: 1) analyzing phase angles which may result in the implementation of an Operating Plan to adjust generation or curtail transactions so that a Transmission facility may be returned to service, or 2) evaluating the impact of a modified Contingency resulting from the status change of a Special Protection Scheme from enabled/in service to disabled/out of service.~~

~~Rationale for Applicability Changes:~~

~~Changes were made to applicability based on IRO FYRT recommendation to address the need for UVLS and UFLS information in the data specification.~~

~~The Interchange Authority was removed because activities in the Coordinate Interchange standards are performed by software systems and not a responsible entity. The software, not a functional entity, performs the task of accepting and disseminating interchange data between entities. The Balancing Authority is the responsible functional entity for these tasks.~~

~~The Planning Coordinator and Transmission Planner were removed from Draft 2 as those entities would not be involved in a data specification concept as outlined in this standard.~~

~~Rationale:~~

~~Proposed Requirement R1, Part 1.1:~~

~~Is in response to issues raised in NOPR paragraph 67 on the need for obtaining non-BES and external network data necessary for the Reliability Coordinator to fulfill its responsibilities.~~

~~Proposed Requirement R1, Part 1.2:~~

~~Is in response to NOPR paragraph 78 on relay data.~~

~~Proposed Requirement R3, Part 3.3:~~

~~Is in response to NOPR paragraph 92 where concerns were raised about data exchange through secured networks.~~

~~Corresponding changes have been made to proposed TOP-003-3.~~

Standard Development Timeline

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

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title:** Operational Reliability Data
2. **Number:** TOP-003-54
3. **Purpose:** To ensure that the Transmission Operator and Balancing Authority have data needed to fulfill their operational and planning responsibilities.
4. **Applicability:**
 - 4.1. Transmission Operator
 - 4.2. Balancing Authority
 - 4.3. Generator Owner
 - 4.4. Generator Operator
 - 4.5. Transmission Owner
 - 4.6. Distribution Provider
5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements and Measures

- R1. Each Transmission Operator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
 - 1.1. A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data as deemed necessary by the Transmission Operator.
 - 1.2. Provisions for notification of current Protection System and ~~Special Protection System~~ Remedial Action Scheme (RAS) status or degradation that impacts System reliability.
 - 1.2.1.3. Provisions for notification of BES generating unit-specific design specification or minimum historical performance during cold weather, and expected BES generating unit operation limitations during local forecasted cold weather.
 - 1.3.1.4. A periodicity for providing data.
 - 1.4.1.5. The deadline by which the respondent is to provide the indicated data.
- M1. Each Transmission Operator shall make available its dated, current, in force documented specification for data.
- R2. Each Balancing Authority shall maintain a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. The data

specification shall include, but not be limited to: *[Violation Risk Factor: Lower]* *[Time Horizon: Operations Planning]*

- 2.1. A list of data and information needed by the Balancing Authority to support its analysis functions and Real-time monitoring.
 - 2.2. Provisions for notification of current Protection ~~System and Special Protection~~ System Remedial Action Scheme status or degradation that impacts System reliability.
 - 2.3. A periodicity for providing data.
 - 2.4. The deadline by which the respondent is to provide the indicated data.
- M2.** Each Balancing Authority shall make available its dated, current, in force documented specification for data.
- R3.** Each Transmission Operator shall distribute its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *[Violation Risk Factor: Lower]* *[Time Horizon: Operations Planning]*
- M3.** Each Transmission Operator shall make available evidence that it has distributed its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.
- R4.** Each Balancing Authority shall distribute its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. *[Violation Risk Factor: Lower]* *[Time Horizon: Operations Planning]*
- M4.** Each Balancing Authority shall make available evidence that it has distributed its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, or e-mail records.
- R5.** Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall satisfy the obligations of the documented specifications using: *[Violation Risk Factor: Medium]* *[Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*
- 5.1. A mutually agreeable format
 - 5.2. A mutually agreeable process for resolving data conflicts
 - 5.3. A mutually agreeable security protocol

- M5.** Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations of the documented specifications. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority”
As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority”
(CEA) means NERC or the Regional Entity, or any entity as otherwise designated
by an Applicable Governmental Authority, in their respective roles of monitoring
and/or enforcing compliance with mandatory and enforceable the NERC
Reliability Standards in their respective jurisdictions.

~~1.2.~~ Data Evidence Retention:

~~1.3.~~ 1.2. The following evidence retention period(s) identify the period of time an
entity is required to retain specific evidence to demonstrate compliance. For
instances where the evidence retention period specified below is shorter than
the time since the last audit, the Compliance Enforcement Authority may ask an
entity to provide other evidence to show that it was compliant for the full time
period since the last audit.

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

Each Transmission Operator shall retain its dated, current, in force, documented
specification for the data necessary for it to perform its Operational Planning
Analyses, Real-time monitoring, and Real-time Assessments in accordance with
Requirement R1 and Measurement M1 as well as any documents in force since
the last compliance audit.

Each Balancing Authority shall retain its dated, current, in force, documented
specification for the data necessary for it to perform its analysis functions and
Real-time monitoring in accordance with Requirement R2 and Measurement M2
as well as any documents in force since the last compliance audit.

Each Transmission Operator shall retain evidence for three calendar years that it
has distributed its data specification to entities that have data required by the
Transmission Operator’s Operational Planning Analyses, Real-time monitoring,
and Real-time Assessments in accordance with Requirement R3 and
Measurement M3.

Each Balancing Authority shall retain evidence for three calendar years that it
has distributed its data specification to entities that have data required by the
Balancing Authority’s analysis functions and Real-time monitoring in accordance
with Requirement R4 and Measurement M4.

Each Balancing Authority, Generator Owner, Generator Operator, Transmission
Operator, Transmission Owner, and Distribution Provider receiving a data
specification in Requirement R3 or R4 shall retain evidence for the most recent

90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R5 and Measurement M5.

~~If a responsible entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or 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.~~

1.4.1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.5.1.4. **Additional Compliance Information**
None.

-Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Low ~~er~~	The Transmission Operator did not include ~~two or fewer~~ of the parts (Part 1.1 through Part 1. ~~54~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include ~~two~~ ~~three~~ of the parts (Part 1.1 through Part 1. ~~54~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include ~~four~~ ~~three~~ of the parts (Part 1.1 through Part 1. ~~54~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include ~~any~~ ~~four~~ of the parts (Part 1.1 through Part 1. ~~54~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Transmission Operator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	Low <u>er</u>	The Balancing Authority did not include one of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include two of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include three of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include four of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. OR, The Balancing Authority did not have a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.
For the Requirement R3 and R4 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R3	Operations Planning	Low <u>er</u>	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to four or more entities, or more than 15% of the entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R4	Operations Planning	Lower	The Balancing Authority did not distribute its data specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to two entities, or more than 5% and less than or equal to 10% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to three entities, or more than 10% and less than or equal to 15% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to four or more entities, or more than 15% of the entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet one of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet two of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet three of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP-003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07

Guidelines and Technical Basis

Rationale:

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

Rationale for Definitions:

~~Changes made to the proposed definitions were made in order to respond to issues raised in NOPR paragraphs 55, 73, and 74 dealing with analysis of SOLs in all time horizons, questions on Protection Systems and Special Protection Systems in NOPR paragraph 78, and recommendations on phase angles from the SW Outage Report (recommendation 27). The intent of such changes is to ensure that Real-time Assessments contain sufficient details to result in an appropriate level of situational awareness. Some examples include: 1) analyzing phase angles which may result in the implementation of an Operating Plan to adjust generation or curtail transactions so that a Transmission facility may be returned to service, or 2) evaluating the impact of a modified Contingency resulting from the status change of a Special Protection Scheme from enabled/in-service to disabled/out-of-service.~~

Rationale for R1:

~~Changes to proposed Requirement R1, Part 1.1 are in response to issues raised in NOPR paragraph 67 on the need for obtaining non-BES and external network data necessary for the Transmission Operator to fulfill its responsibilities.~~

~~Proposed Requirement R1, Part 1.2 is in response to NOPR paragraph 78 on relay data. The language has been moved from approved PRC-001-1.~~

~~Corresponding changes have been made to Requirement R2 for the Balancing Authority and to proposed IRO-010-2, Requirement R1 for the Reliability Coordinator.~~

Rationale for R5:

~~Proposed Requirement R5, Part 5.3 is in response to NOPR paragraph 92 where concerns were raised about data exchange through secured networks.~~

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:		Revise the Applicable Facilities of MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 Standards to comprehensively include all types of dynamic reactive resources (including static var systems and FACTS) and DC transmission systems used to provide Essential Reliability Services in the Bulk Electric System.	
Date Submitted:		February 24, 2020	
SAR Requester			
Name:		Hari Singh – Chair, System Analysis & Modeling Subcommittee (SAMS)	
Organization:		Xcel Energy	
Telephone:		303-571-7095	Email: hari.singh@xcelenergy.com
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Dynamic reactive resources used to provide Essential Reliability Services (ERS) in the BES include generation resources (rotating machine and inverter-based) as well as transmission connected dynamic reactive resources (power-electronics based). Existing reliability standards for verifying the capability, modeling and performance of dynamic reactive resources are only applicable to Facilities comprising generation resources. Augmenting the applicability of these standards to include (non-generation) transmission-connected reactive resources – both rotating machine (i.e. synchronous condenser) and power-electronics based – will enhance the BES reliability by ensuring that the capability, models and performance is verified and validated for all varieties of dynamic reactive resources utilized in providing ERS in the BES.			

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
Augment the “Applicability – Facilities” and “Applicability-Functional Entities” sections in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards to address (non-generation) transmission-connected dynamic reactive resources – both rotating machine (i.e. synchronous condenser) and power-electronics based. Also modify Requirements (including applicable attachments) as needed to ensure they continue to address the additional Facilities. As needed, also define new Glossary Terms for all or some of the transmission-connected dynamic reactive devices noted in the SAMS white-paper “ <i>Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards</i> ”.
Project Scope (Define the parameters of the proposed project):
Revise the “Applicability – Facilities” section, “Applicability – Functional Entities” section, and Requirements (including applicable attachments) as needed in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards to comprehensively address all varieties of transmission-connected dynamic reactive resources that are utilized in providing ERS in the BES.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification ¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g. research paper) to guide development of the Standard or definition):
The “Applicability – Facilities” and “Applicability-Functional Entities” sections in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards will be revised to address (non-generation) transmission-connected dynamic reactive resources based on the recommendations summarized in Table 1 of the SAMS white-paper “ <i>Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards</i> ”. The white-paper also provides the technical justifications for the recommended revisions and the associated reliability benefits. Also modify Requirements (including applicable attachments) as needed to ensure they continue to address the additional Facilities. As needed, also define new Glossary Terms for all or some of the transmission-connected dynamic reactive devices noted as items 1.a – 1.j in the Additional Considerations section of the SAMS white-paper.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Unknown
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g. Dispersed Generation Resources):
Power-electronics based transmission-connected reactive resources – also known as FACTS (Flexible AC Transmission System) devices – such as: Static Var Compensator (SVC), Static Synchronous Compensator (STATCOM), HVDC Links (LCC or VSC).
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g. Transmission

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Transmission Owners in addition to the existing Functional Entities
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
<i>"Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards"</i> white-paper approved by SAMS members.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?
PRC-019 SAR requested by SPCS and PRC-024 SAR requested by IRPTF
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
No viable alternatives were found by SAMS.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those 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.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project 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
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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
<i>e.g.</i> NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☒ Draft SAR reviewed by NERC Staff ☒ Draft SAR presented to SC for acceptance ☒ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:		Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security	
Date Submitted:		March 4, 2020	
SAR Requester			
Name:		Soo Jin Kim, Senior Manager of Standards Development	
Organization:		NERC	
Telephone:		404.831.4765	Email: Soo.jin.kim@nerc.net
SAR Type (Check as many as apply)			
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)		
☒ Revision to Existing Standard	☐ Variance development or revision		
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)		
☐ Withdraw/retire an Existing Standard			
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation	☐ NERC Standing Committee Identified		
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated		
☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified		
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The project will increase reliability through consistent supply chain protections to low impact BES Cyber Systems. The NERC Supply Chain Risk Assessment Report (December 2019) found that 87% of all BES Cyber Asset locations have low impact BES Cyber Systems, and many of these locations have external connectivity. Currently the systems at these locations would not be subject to the current Supply Chain Standards, CIP-005-6, CIP-010-3 and CIP-013-1. The impact to the reliability of the BES could be significant if multiple owners and operators allow third-party access to their facilities and the associated BES Cyber Systems possess a common supply chain vulnerability. This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
This project will address the NERC Board resolution adopted at its February 2020 to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect			

Requested information
known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Project Scope (Define the parameters of the proposed project):
This project will address recommendations from the NERC Supply Chain Risk Assessment Report. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):
Revise CIP-003-8 to include policies for low impact BES Cyber Systems at locations that allow 3rd party remote access to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
Project 2016-02 Modifications to CIP Standards for changes to definitions, standards or requirements. Project 2019-02 BES Cyber Systems Information Access Management for changes to definitions, standards or requirements.

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

None at this time.

Reliability Principles

Does this proposed standard development project support at least one of the following Reliability Principles ([Reliability Interface Principles](#))? Please check all those 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.

Market Interface Principles

Does the proposed standard development project 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
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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐ DRAFT SAR approved for posting by the SC	☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information

SAR Title:	Revisions to CIP <u>Reliability</u> sStandards to address Cyber Security <u>of</u> Communications between Control Centers		
Date Submitted:	March 4, 2020		
SAR Requester			
Name:	Soo Jin Kim, Manager of Standards Development		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net
SAR Type (Check as many as apply)			
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)		
☒ Revision to Existing Standard	☐ Variance development or revision		
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)		
☐ Withdraw/retire an Existing Standard			
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☒ Regulatory Initiation	☐ NERC Standing Committee Identified		
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated		
☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified		
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
~~The project will address a directive issued by~~ On January 23, 2020, the Federal Energy Regulatory Commission (FERC) ~~in-issued~~ Order No. 866 <u>approving CIP-012 and directing NERC</u> to develop modifications to ~~the CIP Reliability Standards~~ CIP-012 to require protections regarding the availability of communications links and data communicated between the ~~b~~Bulk ~~e~~Electric ~~s~~System (<u>BES</u>) Control Centers.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
~~This project will address the concerns of FERC outlined in Order No. 866.~~ <u>The purpose of this project is to address the Commission directive in Order No. 866 to develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between BES Control Centers. These revisions will</u>			

Requested information	
	<u>improve the security posture of responsible entities by clarifying expectations regarding communication between Control Centers, thereby ensuring the exchange of operational data and addressing the potential risk of loss of data.</u>
	Project Scope (Define the parameters of the proposed project): <u>This project will address the directive in Order No. 866. The proposed project will address the Commission directive regarding the availability of communication links and data communicated between BES Control Centers via development of modifications to CIP-012-1 as outlined in Order No. 866. The work will include development of Violation Risk Factors, Violation Severity Levels and an Implementation Plan for the modified Standard.</u>
	Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification ¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition): <u>The SDT shall address the Order No. 866 directive by developing modifications to Reliability Standard CIP-012-1. The Commission directed the following:</u> <u>Per paragraph 3, "[T]he Commission directs NERC to develop modifications to the CIP Reliability Standards to require protections regarding the <i>availability of communication links and data communicated between bulk electric system Control Centers.</i>"</u> In Order No. 866, FERC stated that "maintaining the availability of communication networks and data should include provisions for incident recovery and continuity of operations in a responsible entity's compliance plan." FERC recognized that the redundancy of communication links cannot always be guaranteed, and acknowledged there should be plans for both recovery of compromised communication links and use of backup communication capability. See Order No. 866 at PP 35-36.
	Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project): <u>Cost impact is unknown at this time.</u> <u>No additional project costs outside of the time and resources required to serve on the Standard Drafting Team are expected. Cost impact of implementation of the proposed Standard is dependent upon the method(s) by which a Responsible Entity chooses to meet any additional Requirements. However, a question will be asked during the comment period to ensure cost aspects are considered.</u>
	Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources): Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, ~~Distribution Provider~~ , Generator Owner, Generator Operator
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
<u>None.</u>
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
Project 2016-02 Modifications to CIP ~~Standards~~ , and <u>Project Standards, Project 2019-02 BES Cyber Systems Information Access Management, and 2020-03 Supply Chain Low Impact Revisions</u> are both active CIP projects.
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time.

Reliability Principles
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those 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.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project 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
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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	FAC-001-3 Facility Interconnection Requirements; FAC-002-2, Facility Interconnection Studies		
Date Submitted:	June 10, 2020		
SAR Requester			
Name:	Allen Shriver, Chair Jeffery Billo, Vice Chair		
Organization:	Inverter-Based Resource Performance Task Force (IRPTF)		
Telephone:	Allen: 561-904-3234 Jeffery: 512-248-6334	Email:	Allen.Shriver@NextEraEnergy.com Jeff.Billo@ercot.com
SAR Type (Check as many as apply)			
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)		
☒ Revision to Existing Standard	☐ Variance development or revision		
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)		
☐ Withdraw/retire an Existing Standard			
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation	☒ NERC Standing Committee Identified		
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated		
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified		
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The NERC Inverter-based Resource Performance Task Force (IRPTF) undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or improvements based on the work and findings of the IRPTF. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in a white paper. The "IRPTF Review of NERC Reliability Standards White Paper" was approved by the Operating Committee and the Planning Committee in March 2020. Among the findings noted in the white paper, the IRPTF identified issues with FAC-001-3 and FAC-002-2 that should be addressed. The purpose of FAC-001-3 is to ensure that Facility interconnection requirements exist for Transmission Owners and Generator Owners when connecting new or materially modified facilities. The purpose of FAC-002-2 is to ensure studies are performed to analyze the impact of interconnecting new or materially			

Requested information
modified facilities on the Bulk Electric System (BES). An ambiguity exists in these standards in regards to the term “materially modified” and which entity is responsible for making such a determination. Hence, these standards need to be modified to address this issue.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
This SAR proposes to revise FAC-001-3 and FAC-002-2 to clarify requirements related to material modifications of Facilities.
Project Scope (Define the parameters of the proposed project):
The proposed scope of this project is as follows: a. Consider ways to clarify which entity is responsible for making the determination of what is considered to be a material modification to a Facility. b. Consider requiring Facility owners to notify affected entities when making a material modification to a Facility. c. Consider changing the term “materially modifying” to avoid confusion with similar terminology that is used for a different purpose in the FERC Open Access Transmission Tariff. d. Consider other manners in which to clarify existing requirements to ensure new or materially modified Facilities on the Bulk Electric System (BES) are adequately accounted for to ensure reliability.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification ¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):
Both FAC-001-3 and FAC-002-2 imply that the term “materially modified” should be used to distinguish between facility changes that are required to be studied and those that need not be studied. However, there is not a requirement for any entity to determine what changes are to be considered materially modifying and Facility owners are not required to notify potentially affected entities of these changes. This has led to confusion and potential reliability issues within industry. For example, a Transmission Planner may consider an inverter-based resource (IBR) control system software change to be materially modifying, but if the Generator Owner does not consider such a change to be materially modifying they will not notify the Transmission Planner of the change. While the existing standards do require coordination and cooperation between a Facility owner and the Transmission Planner or Planning Coordinator when a new or materially modified interconnection Facility is connected to their system, for example FAC-002-2 Requirement R5, neither standard specifies what entity is responsible for determining what is considered to be a material modification. Further, the existing language is unclear about whether these requirements only apply when a different entity is proposing to interconnect to a Facility owner’s Facility or if they also apply to the Facility owner’s new or modified Facility.

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Additionally, in FERC-jurisdictional areas, the term “Materially Modification” refers to a new generation project’s impact on other generators in the interconnection queue. This has led to widespread confusion across the industry regarding the correct application of these terms related to the FERC Open Access Transmission Tariff (OATT) implementation and the NERC Reliability Standards requirements. The application of these terms is different between the FERC process and the NERC Reliability Standards (specifically FAC-001-3 and FAC-002-2). For example, if a Generator Owner changes out the inverters on an existing solar PV resource, the change may have no impact on other generators in the interconnection queue, and thus would not be considered a Material Modification under the FERC OATT rules. But such a change could have reliability impacts on the system that should be studied in accordance with FAC-002-2. The Standards Drafting Team should consider changing the term to avoid this confusion. FAC-001-3 and FAC-002-2 should be modified to clarify the use of “materially modifying”, particularly as it relates to compliance with the standards.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The SAR proposes to clarify and address gaps in the requirements in FAC-001-3 and FAC-002-2. The cost impact is unknown.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):
The frequency of change of components could be higher for IBRs and the magnitude of such changes could vary. For example, due to a rapid change in wind turbine generator (WTG) technology, it is a common practice to re-power an existing wind power plant with bigger blades while keeping the same electrical generator and converter systems (for both Type 3 and Type 4 WTGs). This may be considered a material modification since a new set of bigger blades (e.g., 93 m to 208 m) can produce more power at a lower wind speed. However, the nameplate rating of the plant will remain unchanged. From an interconnection requirements’ perspective, it is the electrical generator and converter system that impacts the majority of the steady-state, short-circuit, and dynamic characteristics and therefore will be mostly unchanged. Therefore, the question remains if these sort of repowering projects should be studied under FAC-002-2 R1 and which entity should make that determination.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Planning Coordinator, Transmission Planner, Generator Owner, Transmission Owner, Distribution Provider
Do you know of any consensus building activities² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This issue was captured in the “IRPTF Review of NERC Reliability Standards White Paper” which was approved by the Operating Committee and the Planning Committee.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
N/A
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
The IRPTF did not identify any alternatives since there are ambiguities in the existing language for FAC-001-3 and FAC-002-2 that need to be clarified.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those 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.

Market Interface Principles	
Does the proposed standard development project 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
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

Identified Existing or Potential Regional or Interconnection Variances

Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).

☐ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐ DRAFT SAR approved for posting by the SC	☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:		MOD-026-1 Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions, MOD-027-1 Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions	
Date Submitted:		June 10, 2020	
SAR Requester			
Name:		Allen Shriver, Chair Jeffery Billo, Vice Chair	
Organization:		Inverter-Based Resource Performance Task Force (IRPTF)	
Telephone:		Allen: 561-904-3234 Jeffery: 512-248-6334	
Email:		Allen.Schrivier@NextEraEnergy.com Jeff.Billo@ercot.com	
SAR Type (Check as many as apply)			
☒ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The NERC Inverter-based Resource Performance Task Force (IRPTF) undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or improvements based on the work and findings of the IRPTF. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in a white paper. The "IRPTF Review of NERC Reliability Standards White Paper" was approved by the Operating Committee and the Planning Committee in March 2020. Among the findings noted in the white paper, the IRPTF identified issues with MOD-026-1 and MOD-027-1 that should be addressed.			

Requested information
MOD-026-1 and MOD-027-1 require, among other things, GOs to provide verified dynamic models to their Transmission Planner (TP) for the purposes of power system planning studies. Both standards contain language that is specific to synchronous generators and is not applicable to inverter-based resources (IBRs). For example, sub-requirement 2.1.3 in MOD-026-1 states that each verification shall include “model structure and data including, but not limited to reactance, time constants, saturation factors, total rotational inertia...” The standards should be revised to clarify the applicable requirements for synchronous generators and IBRs. For example, total rotational inertia should not be required for IBRs, while voltage ride-through control settings should only be required of IBRs and not synchronous generators. Additionally, to some degree, all dynamic model parameters affect the response of a represented resource in dynamic simulations performed by power engineers. Accurate model response is required for the engineers to adequately study system conditions. Hence, it is crucial that all parameters in a model be verified in some way. However, a significant number of parameters in the models are not verified in the typical verification tests used to comply with MOD-026-1 and MOD-027-1. For example, the test currently used to comply with MOD-026-1 does not verify the model parameters associated with voltage control behavior during large disturbance conditions.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?): This SAR proposes to revise MOD-026-1 and MOD-027-1 and/or create a new standard to clarify requirements related to IBRs and to require sufficient model verification to ensure accurate generator representation in dynamic simulations.
Project Scope (Define the parameters of the proposed project): The proposed scope of this project is as follows: a. Update requirement language to better reflect all types of generation resources and not just synchronous resources. b. Consider ways to require sufficient model verification to ensure accurate generator representation in dynamic simulations of typical phenomena that would be studied by power system engineers, including large disturbances.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition): NERC MOD-026-1 focuses on verification of data for generator excitation control system or plant volt/var control functions and MOD-027-1 focuses on verification of data for turbine-governor and load control or active power-frequency control functions. Specifically, MOD-026-1 states in footnote 1 that the excitation control system for aggregate generating plants (i.e., wind and solar PV) includes the volt/var control system including the voltage regulator and reactive power control system controlling and coordinating

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information

plant voltage and associated reactive capable resources. This language is slightly ambiguous on whether the verification activities include the inverter-level parameter values of the dynamic models. Various testing engineers and entities have stated that they are uncertain as to whether the standard applies to the plant-level parameters or the aggregate representation of the inverter-level settings.

Most commonly, verification test reports for inverter-based resources involve a small set of small disturbance tests including, but not limited to, the following:

- Capacitor switching test
- Plant-level voltage or reactive power reference step test
- Plant-level frequency reference step test
- Plant-level frequency play-in or step test

These tests do not perturb the generating resource such that the parameter values that dictate the large disturbance behavior of the resource are verified in any way. While some incorrect model parameters may be identified during these tests, the tests do not verify that the parameters selected for the model accurately capture the full dynamic behavior of the resource. This gives a false impression to TPs and PCs that the full set of parameters are verified for use in planning studies.

This issue is one of the predominant reasons why ride-through operation modes such as momentary cessation were able to persist and promulgate in IBRs without the knowledge of planners and system operators until the Blue Cut Fire and Canyon 2 Fire events exposed them. The dynamic models did not accurately represent this large disturbance behavior due to the model deficiency and because certain key parameters that govern large disturbance response were incorrectly parameterized. However, many of the same plants that entered momentary cessation mode during these events were able to provide verification reports that demonstrated that the small disturbance behavior driven mainly by plant-level control settings reasonably matched modeled performance in compliance with these standards.

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

The SAR proposes to clarify and address gaps in the requirements in MOD-026-1 and MOD-027-1. The cost impact is unknown.

Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):

The abovementioned reliability gap exists for both synchronous generators and IBRs. However, it is potentially more severe for IBRs since their behavior is based more on programmable control functions than for synchronous generators which have behavior that is based more on the physical characteristics of the machine. Additionally, the IRPTF noted that it is not feasible to stage large disturbances for verification purposes, so other methods for verification of model performance under large disturbance conditions may need to be developed.

To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission

Requested information
Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Transmission Planner, Generator Owner, Planning Coordinator
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This issue was captured in the “IRPTF Review of NERC Reliability Standards White Paper” which was approved by the Operating Committee and the Planning Committee. Additionally, the issue was discussed in the IRPTF-produced “Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources” reliability guideline.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
N/A
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
The IRPTF did not identify any alternatives since there are gaps in the existing language for MOD-026-1 and MOD-027-1 that need to be resolved.

Reliability Principles
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those 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.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project 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
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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

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%			
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%			

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
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%			
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%			

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
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%			
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%			

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
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%			
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	Proect 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%			

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
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%			
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		

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
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		
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%			
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%			

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
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		
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		

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
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%			
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		

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
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%			
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%			

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
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		
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		

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
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		
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
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

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
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%			
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.]		The majority of RSC member 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%			

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
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%			
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.

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
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		
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: 79.12% 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%		--	
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	

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
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: 89.03%/83.46% 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.
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 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% Approval: 42.27%	Negative--8/14/14	Negative	
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	(Sudden Pressure Relays) - PRC-005-X	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 %	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		

Last RSC Meeting

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
						Approval: 76.12%/74.23%/75.67 %/85.49%/75.96%/78. 67%/48.73%/78.87%/ 87.03%/93.34%/90.13 %	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 9/18/14		
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%	Negative--10/1/14		
						Approval: 46.73%			
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%	Affirmative--10/1/14		
						Approval: 53.02%			
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: 84.40% 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		
498	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Additional Ballot	10/7/2014	10/16/2014	Quorum: 81.91%/82.12% Approval: 94.92%/94.37%	Affirmative--10/14/14		
499	Project 2014-02	Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions	Additional Ballot	10/8/2014	10/17/2014	Quorum: 84.63%/84.15%/84.15 %/83.90%/83.41%/83. 66%/83.96%/84.49%/83. 96%/83.96%/84.22 %/84.49%/84.22% Approval: 93.21%/68.09%/74.25 %/79.91%/85.68%/89. 01%/91.79%/81.34%/96.63%/96.63%/95.52 %/85.93%/98.13%	CIP-003-6 no consensus CIP-010-2 no consensus New Definitions-Affirmative Updated Definitions-Affirmative Implementation Plan-Affirmative Version X Materials-Affirmative Non-binding polls-Affirmative	CIP-003-6 and CIP-010-2 Affirmative	
500	Project 2009-03	Project 2009-03 Emergency Operations	Additional Ballot	10/10/2014	10/20/2014	Quorum: 80.93% Approval: 70.41%	Affirmative--10/17/14		
501	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards (IRO-001-4, IRO-002-4, IRO-010-2, two Definitions, and Implementation Plan)	Final Ballot	10/10/2014	10/20/2014	Quorum: 90/77%/89.97%/89.97 %/88.39%/88.39% Approval: 82.64%/85.96%/86.22 %/94.07%/91.84%	Affirmative--10/17/14		
502	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards (TOP-002-4, TOP-003-3, IRO-008-2, IRO-014-3, and IRO-017-1)	Final Ballot	10/10/2014	10/20/2014	Quorum: 89.71%/88.39%/89.71 %/89.71%/89.97% 84.76%/86.55%/83.73 %/89.88%/82.58%	Affirmative--10/17/14		
503	Project 2007-11	Project 2007-11 Disturbance Monitoring	Additional Ballot	10/10/2014	10/21/2014	Quorum: 77.69% Approval: 71.38%	Affirmative--10/17/14		
504	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Additional Ballot	10/10/2014	10/22/2014	Quorum: 85.13%/83.29% Approval: 94.75%/93.98%	Affirmative--10/20/14		
505	Project 2014-03	Project 2007-17.3 (PRC-005-X) Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays)	Final Ballot	10/20/2014	10/29/2014	Quorum: 88.25% Approval: 74.14%	Affirmative--10/28/14		
506	Project 2014-03	Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	Final Ballot	10/28/2014	11/6/2014	Quorum: 87.53% Approval: 83.12%	Affirmative--10/31/14		
507	Project 2007-11	Project 2007-11 Disturbance Monitoring	Final Ballot	10/28/2014	11/6/2014	Quorum: 81.89% Approval: 68.51%	Affirmative--10/31/14		
508	Project 2007-11	Project 2010-05.2 Phase 2 of Special Protection Systems	Final Ballot	10/28/2014	11/6/2014	Quorum: 85.41% Approval: 73.33%	Negative--10/14/14		
509	Project 2007-11	Project 2009-03 Emergency Operations	Final Ballot	10/28/2014	11/6/2014	Quorum: 87.19% Approval: 73.20%	Affirmative--10/17/14		

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
510	Project 2007-11	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Final Ballot	10/28/2014	11/6/2014	Quorum: 89.49%/87.66%/87.08 % Approval: 92.91%/92.15%/95.62 %	Affirmative--10/20/14		
511	Project 2014-03	Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions	Final Ballot	10/28/2014	11/6/2014	Quorum: 87.56%/87.32%87.07 %/87.56%/87.80%87.5 6%86.59% Approval: 83.84%/95.34%/86.00 %/95.35%91.17%/83.8 8%/95.40%/92.76%	CIP-003-6 no consensus CIP-010-2 no consensus New Definitions-Affirmative Updated Definitions-Affirmative Implementation Plan-Affirmative Version X Materials-Affirmative Non-binding polls-Affirmative		
512	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards	Additional Ballot	11/4/2014	11/10/2014	Quorum: 78.36% Approval: 60.21%	Affirmative--11/4/14		
513	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	Additional Ballot	11/12/2014	11/21/2014	Quorum: 79.73% Approval: 77.29%	Affirmative--11/21/14		
514	Project 2014-03	Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings	Additional Ballot	11/14/2014	11/24/2014	Quorum: 79.83% Approval: 67.39%	Affirmative--10/1/14		
515	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	Final Ballot	12/5/2014	12/16/2014	Quorum: 84.27% Approval: 78.05%	Affirmative--12/12/14		
516	Project 2014-03	Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings	Final Ballot	12/5/2014	12/16/2014	Quorum: 84.81% Approval: 68.08%	Affirmative--12/15/14		
517	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Initial Ballots	12/10/2014	12/23/2014	Quorum: 79.38%/79.72%/79.60 % Approval: 92.69%/93.55%/93.67 %	Affirmative--12/22/14		
518	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards	Additional Ballot	12/19/2014	1/7/2015	Quorum: 80.47% Approval: 72.43%	Affirmative--1/6/15		
519	Project 2014-02	2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions	Additional Ballot	12/30/2014	1/9/2015	Quorum: 81.22%/81.71%/81.46 %/81.71%/81.71%/81. 22%/81.71%/81.46% Approval: 81.92%/98.89%/98.86 %/88.13%/98.89%/86. 02%/89.63%/97.21%	CIP-003-7 Binding and non-binding polls-no consensus CIP-003-7 Definition-Affirmative CIP-010-7 Binding and non-binding polls- Affirmative CIP-010-7 Definition- Affirmative CIP-004-7 Binding and non-binding polls – Affirmative CIP-007-7 Binding and non-binding polls –Affirmative CIP-011-7 Binding and non-binding polls –Affirmative CIP Implementation Plan- Affirmative 1/8/2015		
520	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards - TOP-001-3	Final Ballots	1/15/2015	1/21/2015	Quorum: 84.70% Approval: 72.69%	Affirmative--1/6/15		
521	Project 2014-01	2014-01 - Standards Applicability for Dispersed Generation Resources - PRC-005-5	Initial Ballots	1/12/2015	1/22/2015	Quorum: 77.93% Approval: 93.74%	Affirmative--1/22/15		
522	Project 2014-01	2014-01 - Standards Applicability for Dispersed Generation Resources - PRC-001-1.1(iii), PRC-019-2, and PRC-024-2	Final Ballots	1/13/2015	1/22/2015	Quorum: 89.27%/89.30%/89.52 % Approval: 93.99%/94.03%/95.82 %	Affirmative--1/22/15		
523	Project 2014-02	2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions CIP-003-7, CIP-004-7, CIP-010-3, and CIP-011-3	Final Ballot	1/23/2015	2/2/2015	Quorum: 84.15%/84.39%/84.15 %/84.39%/84.39%/83. 90%/84.39%/83.66% Approval: 79.76%/98.94%/98.94 %/86.76%/98.93%/84. 07%/90.10%/97.32%	Affirmative--1/29/15		
524	Project 2014-01	2014-01 - Standards Applicability for Dispersed Generation Resources - PRC-005-5	Final Ballot	3/2/2015	3/11/2015	Quorum: 83.52% Approval: 98.03%	Affirmative--1/22/15		
525	Project 2010-14.1	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Additional Ballot	3/6/2015	3/16/2015	Quorum: 77.29% Approval: 59.30%	Negative--3/13/2015		
526	Project 2008-02.2	Project 2008-02.2 Phase 2 of Undervoltage Load Shedding (UVLS): Misoperations	Initial Ballot	3/27/2015	4/7/2015	Quorum: 79.93% Approval: 84.31%	Affirmative--3/31/15		

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
527	Project 2014-04	Project 2014-04 Physical Security	Initial Ballot	3/31/2015	4/9/2015	Quorum: 88.33% Approval: 89.95%	Affirmative--3/31/15		
528	Project 2008-02.2	Project 2008-02.2 Phase 2 of Undervoltage Load Shedding (UVLS): Misoperations	Final Ballot	4/17/2015	4/27/2015	Quorum: 84.86% Approval: 89.63%	Affirmative--3/31/15		
529	Project 2014-04	Project 2014-04 Physical Security	Final Ballot	4/20/2015	4/29/2015	Quorum: 92.00% Approval: 92.35%	Affirmative--3/31/15		
530	Project 2007-06	Project 2007-06 System Protection Coordination	Additional Ballot	5/6/2015	5/15/2015	Quorum: 81.79% Approval: 39.63%	Negative--5//13/15		
531	Project 2015-06	2015-06 Interconnection Reliability Operations and Coordination	Initial Ballot	6/29/2015	7/8/2015	Quorum: 75.23%/84.00% Approval: 90.35%/97.50%	Affirmative--7/7/15		
532	Project 2015-04	2015-04 Alignment of Terms	Initial Ballot	7/17/2015	7/27/2015	Quorum: 90.43%/91.17%/91.10 %/91.01%/91.10%/91.17%/91.17%/91.34%/90.97%/91.40%/90.10 %/91.01%/91.07%/91.07%/91.07%/91.34%/91.43%/90.75%/91.34 %/91.01%/91.40%/91.01%/91.01%/91.01%/91.01% Approval: 91.46%/88.57%/86.68 %/97.06%/97.10%/81.06%/80.73%/96.38%/97.03%/69.80%/95.38 %/93.62%/96.83%/97.00%/98.55%/87.37%/89.99%/84.38%/88.06 %/90.37%/97.75%/91.28%/87.71%/89.44%/87.15%/98.24%	Affirmative--7/24/15		
533	Project 2015-06	2015-06 Interconnection Reliability Operations and Coordination	Final Ballots	7/22/2015	7/31/2015	Quorum: 85.98%/90.67%% Approval: 88.23%/96.84%	Affirmative--7/7/15		
534	Project 2010-14.1	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Additional Ballot	8/11/2015	8/20/2015	Quorum: 75.92% Approval: 69.26%	Affirmative--8/17/15		
535	Project 2007-06	Project 2007-06 System Protection Coordination	Additional Ballot	9/2/2015	9/11/2015	Quorum: 84.34% Approval: 69.76%	Affirmative--9/8/15		
536	Project 2007-06	Project 2007-06.2 Phase 2 of System Protection Coordination	Initial Ballot	9/2/2015	9/11/2015	Quorum: 87.16% Approval: 62.55%	Affirmative--9/11/15		
537	Project 2010-14.2.1	Project 2010-14.2.1 Phase 2 of Balancing Authority Reliability-based Controls – BAL-005 and BAL-006	Initial Ballot	9/4/2015	9/14/2015	Quorum: 83.81% Approval: 55.97%	Abstention--9/14/15		
538	Project 2015-04	2015-04 Alignment of Terms	Final Ballot	9/4/2015	9/14/2015	Quorum: 96.81%/97.53%/97.51 %/97.48%/97.51%/97.53%/97.53%/97.11%/97.11%/97.85%/96.80 %/97.12%/97.14%/97.14%/97.14%/97.11%/97.14%/96.80%/97.11 %/97.48%/97.85%/97.48%/97.48%/97.48%/97.48%	Affirmative--7/24/15		

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
						Approval: 93.13%/92.89%/91.33 %/98.07%/98.07%/84. 78%/84.75%/98.30%/ 98.06%/75.63%/95.46 %/94.48%/98.31%/97. 11%/98.57%/90.80%/ 95.60%/90.46%/92.07 %/92.49%/97.81%/92. 84%/91.09%/91.32%/ 90.80%/98.29%	Affirmative--7/24/15		
539	Project 2007-17.4	Project 2007-17.4 PRC-005 FERC Order No. 803 Directive	Initial Ballot	9/4/2015	9/16/2015	Quorum: 86.97%	Affirmative--9/16/15		
540	Project 2010-04.1	Project 2010-04.1 MOD-031 FERC Order No. 804 Directives	Initial Ballot	9/9/2015	9/18/2015	Approval: 96.73%	Affirmative--9/18/15		
541	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Initial Ballot	9/25/2015	10/5/2015	Quorum: 83.70%	N egative--10/2/15		
542	Project 2010-05.3	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Final Ballot	9/29/2015	10/8/2015	Approval: 48.10%	Affirmative--8/17/15		
543	Project 2010-05.3	Project 2007-06 System Protection Coordination	Final Ballot	10/5/2015	10/14/2015	Quorum: 84.28%	Affirmative--9/8/15		
544	Project 2010-05.3	Project 2010-04.1 MOD-031 FERC Order No. 804 Directives	Final Ballot	10/6/2015	10/15/2015	Approval: 74.61%	Affirmative--9/18/15		
545	Project 2007-17.4	Project 2007-17.4 PRC-005 FERC Order No. 803 Directive	Final Ballot	10/15/2015	10/26/2015	Quorum: 89.16%	Affirmative--9/16/15		
546	Project 2010-05.3	Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities	Initial Ballot	10/30/2015	11/9/2015	Approval: 80.94%	Abstention--11/5/15		
547	Project 2010-05.3	Project 2010-14.2.2 Phase 2 of Balancing Authority Reliability-based Controls - BAL-004-2	Initial Ballot	11/3/2015	11/12/2015	Quorum: 84.40%	Affirmative--11/13/15		
548	Project 2015-07	Project 2015-07 Internal Communications Capabilities	Initial Ballot	11/6/2015	11/16/2015	Approval: 98.17%	Affirmative--11/18/15		
549	Project 2007-06.2	Project 2007-06.2 Phase 2 of System Protection Coordination	Additional Ballot	11/10/2015	11/19/2015	Quorum: 88.18%	Affirmative--11/18/15		
550	Project 2010-07.1	Project 2010-07.1 Vegetation Management	Initial Ballot	12/7/2015	12/16/2015	Approval: 53.60%	Negative--12/8/15		
547	Project 2010-05.3	Project 2010-14.2.2 Phase 2 of Balancing Authority Reliability-based Controls - BAL-004-2	Final Ballot	12/8/2015	12/17/2015	Quorum: 83.18%	Affirmative--11/5/15		
551	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Additional Ballot	12/30/2015	1/8/2016	Approval: 57.29%	Affirmative--12/3015		
552	Project 2010-14.2.1	Project 2010-14.2.1 Phase 2 of Balancing Authority Reliability-based Controls -BAL-005 and BAL-006	Additional Ballot	12/31/2015	1/11/2016	Quorum: 83.39%/80.88%	BAL-005-1--Negative--1/10/16 BAL-006--Affirmative--1/10/16 FAC-003-1--Abstention--1/10/16		
553	Project 2010-05.3	Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities	Additional Ballot	1/15/2016	1/25/2016	Approval: 60.39%/92.94%	Affirmative--1/25/16		
554	Project 2010-07.1	Project 2010-07.1 Vegetation Management	Final Ballot	1/29/2016	2/8/2016	Quorum: 82.88%/82.18%	Affirmative--2/1/16		
552	Project 2010-14.2.1	Project 2010-14.2.1 Phase 2 of Balancing Authority Reliability-based Controls -BAL-005 and BAL-006	Final Ballot	1/29/2016	2/8/2016	Approval: 72.13%/68.01%	Affirmative--2/3/15		
551	Project 2010-05.3	Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities	Final Ballot	2/17/2016	2/26/2016	Quorum: 86.35%/86.98%/86.67 %	Affirmative--1/25/16		
552	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Additional Ballot	3/9/2016	3/18/2016	Approval: 75.68%/73.87%	Affirmative--3/10/16		

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
553	Project 2007-06.2	Project 2007-06.2 Phase 2 of System Protection Coordination	Initial Ballot	4/15/2016	4/25/2016	Quorum: 83.39%/83.33% Approval: 80.57%/78.39%	Affirmative--4/20/16		
554	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Final Ballot	4/20/2016	4/29/2016	Quorum: 81.19%/87.15% Approval: 80.36%/93.43%	Affirmative--3/10/16		
555	Project 2015-07	Project 2015-07 Internal Communications Capabilities	Additional Ballot	4/27/2016	5/6/2016	Quorum: 81.03% Approval: 82.64%	Affirmative--5/6/16		
556	Project 2007-06.2	Project 2007-06.2 Phase 2 of System Protection Coordination	Final Ballot	5/17/2016	5/26/2016	Quorum: 88.96%/88.36% Approval: 82.52%/83.37%	Affirmative--4/20/16		
557	Project 2015-07	Project 2015-07 Internal Communications Capabilities	Final Ballot	6/15/2016	6/24/2016	Quorum: 84.52% Approval: 83.25%	Affirmative--5/6/16		
558	Project 2016-01	Project 2016-01 Modifications to TOP and IRO Standards	Initial Ballot	7/25/2016	8/3/2016	Quorum: 84.50%/85.51% Approval: 67.25%/64.59%	Affirmative--8/1/16		
559	Project 2015-08	Project 2015-08 Emergency Operations EOP-005-3 EOP-006-3 EOP-008-2	Initial Ballot	8/4/2016	8/15/2016	Quorum: 80.45%/81.14%/80.79 % Approval: 52.90%/66.87%/84.13 %	Negative--8/4/16		
560	Project 2016-02	Project 2016-02 Modifications to CIP Standards	Initial Ballot	8/26/2016	9/6/2016	Quorum: 85.00%/84.37%/84.62 % Approval: 41.54%/41.77%/30.63 %	Negative--9/6/16		
561	Project 2015-08	Project 2015-08 Emergency Operations EOP-004-4	Initial Ballot	8/30/2016	9/8/2016	Quorum: 82.75% Approval: 80.32%	Affirmative--9/8/16		
562	Project 2015-INT-01	Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)	Initial Ballot	9/2/2016	9/12/2016	Quorum: 75.43% Approval: 91.68%	Affirmative--9/12/16		
563	Project 2016-01	Project 2016-01 Modifications to TOP and IRO Standards	Additional Ballot	10/5/2016	10/14/2016	Quorum: 83.33%/81.79% Approval: 70.77%/68.85%	Affirmative--10/13/16		
564	Project 2015-INT-01	Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)	Final Ballot	10/13/2016	10/24/2016	Quorum: 81.25% Approval: 91.31%	Affirmative--9/12/16		
565	Project 2016-02	Project 2016-02 Modifications to CIP Standards	Additional Ballot	11/23/2016	12/5/2016	Quorum: 76.40%/76.63% Approval: 85.56%/75.54%	Affirmative--12/1/16		
566	Project 2015-08	Project 2015-08 Emergency Operations EOP-005-3 and EOP-006-3	Additional Ballot	11/30/2016	12/9/2016	Quorum: 80.71%/82.43% Approval: 76.93%/77.17%	Affirmative--11/30/16		
567	Project 2015-08	Project 2015-08 Emergency Operations EOP-008-2	Final Ballot	11/30/2016	12/9/2016	Quorum: 93.36% Approval: 93.17%	Affirmative--11/30/16		
568	Project 2016-01	Project 2016-01 Modifications to TOP and IRO Standards	Final Ballot	12/2/2016	12/12/2016	Quorum: 90.74%/90.40% Approval: 74.30%/72.52%	Affirmative--12/2/16		
569	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-7 and Implementation	Final Ballot	12/9/2016	12/19/2016	Quorum: 82.89%/83.14% Approval: 87.95%/83.03%	Affirmative--12/1/16		
570	Project 2015-08	Project 2015-08 Emergency Operations EOP-004-4	Additional Ballot	12/28/2016	1/6/2017	Quorum: 79.47% Approval: 93.55%	Affirmative--1/4/17		
571	Project 2015-08	Project 2015-08 Emergency Operations EOP-005-3, EOP-006-3	Final Ballot	12/28/2016	1/6/2017	Quorum: 91.00%/91.55% Approval: 83.65%/80.56%	Affirmative--1/4/17		
572	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan and 2 Definitions	Initial Ballot	1/16/2017	1/25/2017	Quorum: 77.81%/76.71%/77.26 %/76.71%	Affirmative--1/23/17		

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
						Approval: 81.30%/87.87%/86.75 %/86.47%	Affirmative--1/23/17		
573	Project 2016-03	Project 2016-03 Cyber Security Supply Chain Risk Management	Initial Ballot	2/24/2017	3/6/2017	Quorum: 87.13%	Abstain--3/2/17		
						Approval: 10.36%			
574	Project 2015-08	Project 2015-08 Emergency Operations EOP-004-4	Final Ballot	1/24/2017	2/2/2017	Quorum: 84.46%	Affirmative--1/4/17		
						Approval: 93.80%			
575	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan and 2 Definitions	Final Ballot	1/30/2017	2/8/2017	Quorum: 86.58%/85.48%/86.03 %/85.48%	Affirmative--1/23/17		
						Approval: 78.55%/86.00%/85.81 %/85.54%			
576	SPM	Revisions to the NERC Standards Process Manual	Initial Ballot	4/24/2017	5/3/2017	Quorum: 78.21%			
						Approval: 64.72%			
577	Project 2016-03	Project 2016-03 Cyber Security Supply Chain Risk Management	Additional Ballot	6/6/2017	6/15/2017	Quorum: 76.02%/76.02%/77.21 %	Affirmative--6/8/17		
						Approval: 89.84%/82.92%/88.64 %			
578	Project 2016-03	Project 2016-03 Cyber Security Supply Chain Risk Management	Final Ballot	7/11/2017	7/20/2017	Quorum: 81.59%/81.33%/82.84 %	Affirmative--6/8/17		
						Approval: 88.79%/81.40%/84.19 %			
579	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-2	Initial Ballot	8/2/2017	8/11/2017	Quorum: 79.87%	Affirmative--8/3/17		
						Approval: 72.67%			
580	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Initial Ballot	8/29/2017	9/8/2017	Quorum: 80.45%	Affirmative--9/1/17		
						Approval: 78.79%			
581	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1 Control Center Communication Networks	Initial Ballot	8/14/2017	9/12/2017	Quorum: 80.00%	Affirmative--9/1/17		
						Approval: 42.74%			
582	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Initial Ballot	9/8/2017	10/23/2017	Quorum: 82.71%	Abstain--10/18/17		
						Approval: 30.50%			
583	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-2	Final Ballot	10/20/2017	10/30/2017	Quorum: 88.74%	Affirmative--8/3/17		
						Approval: 73.35%			
584	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Initial Ballot	9/14/2017	10/30/2017	Quorum: 85.40%	Affirmative--10/30/17		
						Approval: 66.78%			
585	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Initial Ballot	11/3/2017	11/13/2017	Quorum: 87.01%/86.90%/86.90 %/85.57%/85.85	Affirmative--11/10/17		
						Approval: 58.12%/63.17%/56.55 %/76.40%/68.59%			
586	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Additional Ballot	11/20/2017	12/11/2017	Quorum:77.10%	Affirmative--12/4/17		
						Approval: 63.91%			
587	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Additional Ballot	10/30/2017	12/13/2017	Quorum: 81.73%	Affirmative--12/4/17		
						Approval: 88.25%			
588	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Final Ballot	1/9/2018	1/18/2018	Quorum: 82.69%	Affirmative--12/4/17		
						Approval: 89.46%			
589	Project 2017-02	Project 2017-02 Modifications to Personnel Performance, Training and Qualifications	Initial Ballot	2/26/2018	3/7/2018	Quorum: 80.93%/81.27%	Affirmative--3/2/18		
						Approval: 97.50%/98.91%			
590	Project 2017-02	Project 2017-02 Modifications to Personnel Performance, Training and Qualifications	Final Ballot	4/3/2018	4/12/2018	Quorum: 84.82%/84.86%	Affirmative--3/2/18		
						Approval: 96.64%/97.88%			
591	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Additional Ballot	2/23/2018	4/23/2018	Quorum: 80%	Affirmative--4/16/18		
						Approval: 26.44%			
592	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Additional Ballot	3/16/2018	4/30/2018	Quorum: 79.50%	Affirmative--4/25/18		
						Approval: 93.31%			
593	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Additional Ballot	3/16/2018	4/30/2018	Quorum:78.06%	Affirmative--4/25/18		
						Approval: 83.71%			
594	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1 Control Center Definition and Implementation Plan	Initial Ballot	3/16/2018	4/30/2018	Quorum: 81.33%/81.54%	Negative--4/25/18		
						Approval: 46.71%/37.98%			
595	Project 2017-06	Project 2017-06 Modifications to BAL-002-2	Initial Ballot	4/27/2018	5/8/2018	Quorum: 81.82%	Abstain--5/7/17		
						Approval: 80%			

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
596	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Additional Ballot	5/18/2018	7/3/2018	Quorum: 75.16% Approval: 68.45%	Affirmative--6/29/18		
597	Project 2017-06	Project 2017-06 Modifications to BAL-002-2	Final Ballot	7/5/2018	7/16/2018	Quorum: 84.42% Approval: 71.85%	Abstain--5/7/17		
598	SPM	Revisions to the NERC Standards Process Manual	Additional Ballot	7/31/2018	8/9/2018	Quorum: 80.34% Approval: 81.95%	Affirmative--8/7/18		
599	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Final Ballot	8/3/2018	8/13/2018	Quorum: 81.55% Approval: 72.55%	Affirmative--4/25/18		
600	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Additional Ballot	9/5/2018	9/14/2018	Quorum: 75.59% Approval: 69.07%	Affirmative--9/5/18		
601	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Initial Ballot	9/28/2018	10/9/2018	Quorum: 78.59% Approval: 55.89%	Affirmative--10/5/18		
602	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-8	Initial Ballot	9/28/2018	10/9/2018	Quorum: 78.77% Approval: 90.06%	Affirmative--10/5/18		
603	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Additional Ballot	10/8/2018	10/17/2018	Quorum: 83.65%/84.08%/83.77 %/84.82%/82.43%/82. 11%/84.08%/83.60%/83.12%/80.98%/83.28 % Approval: 67.65%/67.46%/53.22 %/77.07%/59.02%/59. 79%/75.07%/69.27%/71.98%/69.93%/82.26 %	Affirmative--10/12/18		
604	Project 2018-02	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting	Initial Ballot	10/18/2018	10/22/2018	Quorum: 81.17% Approval: 20.02%	Reject--10/22/18		
605	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Final Ballot	10/11/2018	10/22/2018	Quorum: 86.39% Approval: 66.69%	Affirmative--9/5/18		
606	SPM	Revisions to the NERC Standards Process Manual	Final Ballot	10/7/2018	10/29/2018	Quorum: 85.96% Approval: 81.61%	Affirmative--8/7/18		
607	Project 2018-01	Project 2018-01 Canadian-specific Revisions to TPL-007-2	Initial Ballot	11/6/2018	11/15/2018	Quorum: 77.54%/79.10% Approval: 100%/100%	Affirmative--11/6/18		
608	Project 2018-02	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting	Additional Ballot	11/20/2018	11/29/2018	Quorum: 94.44% Approval: 75.54%	Affirmative--11/20/18		
609	Project 2018-01	Project 2018-01 Canadian-specific Revisions to TPL-007-2	Final Ballot	11/29/2018	12/10/2018	Quorum: 80.43%/82.09% Approval: 100%/100%	Affirmative--11/6/18		
610	Project 2017-01	Project 2017-01 Modifications to BAL-003-1.1	Initial Ballot	1/8/2019	1/17/2019	Quorum: 92.02%/91% Approval: 96.41%/99.04%	Affirmative--1/14/19		
611	Project 2018-02	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting	Final Ballot	1/15/2019	1/22/2019	Quorum: 96.30% Approval: 77.89%	Affirmative--11/20/18		
612	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Initial Ballot	4/3/2019	4/12/2019	Quorum: 86.75%/87.96%/87.80 %/87.58%/87.58%/87. 50%/87.58%/87.34%/87.46%/86.45%/87.34 %/86.77%/87.17%/87. 17%/86.89%/85.71%/85.67%/86.39% Approval: 96.18%/98.88%/97.41 %/97.79%/98.51%/89. 75%/98.53%/96.60%/95.96%/96.60%/95.80 %/98.95%/96.45%/96. 54%/95.90%/88.42%/98.96%/97.69%	Affirmative--4/10/19 for all standards except three. Negative--4/10/19 on following standard: PRC-004-5(i), INT-010-2.1 and FAC-0008-3		
613	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-8	Final Ballot	4/18/2019	4/29/2019	Quorum: 83.64% Approval: 91.44%	Affirmative--10/5/18		

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
614	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Final Ballot	4/3/2019	4/12/2019	Quorum: 90.22%/90.97%/90.85 %/90.94%/90.94%/90. 88%/90.60%/90.26%/ 90.43%/90.32%/90.26 %/90.65%90.13%/90.1 3%/89.84%/90.06%/9 0.03%/89.56% Approval: 95.74%/86.66%/85.94 %/96.64%/97.22%/90. 19%/97.19%/95.47%/ 94.63%/94.34%/94.69 %/96.59%95.28%/95.4 1%94.55%/87.12%/97. 75%/96.57%	Affirmative--4/10/19 for all standards except three.		
615	Project 2018-04	Project 2018-04 Modifications to PRC-024-2	Initial Ballot	5/22/2019	5/31/2019	Quorum: 88.08% Approval: 52.28%	Abstain--5/29/19		
616	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Additional Ballot	6/3/2019	7/17/2019	Quorum: 85.40% Approval: 87.39%	Affirmative--7/15/19		
617	Project 2019-01	Project 2019-01 Modifications to TPL-007-3	Initial Ballot	8/30/2019	9/9/2019	Quorum: 91.44% Approval: 88.81%	Affirmative--9/5/19		
618	Project 2017-01	Project 2017-01 Modifications to BAL-003-1.1	Final Ballot	10/10/2019	10/24/2019	Quorum: 92.96% Approval: 1001%	Affirmative--1/14/19		
619	Project 2018-04	Project 2018-04 Modifications to PRC-024-2	Additional Ballot	10/25/2019	11/4/2019	Quorum: 81.88% Approval: 86.67%	Affirmative--11/4/19		
620	Project 2019-01	Project 2019-01 Modifications to TPL-007-3	Final Ballot	11/13/2019	11/22/2019	Quorum: 94.52% Approval: 78.95%	Affirmative--9/5/19		
621	Project 2017-07	Project 2017-07 Standards Alignment with Registration	Initial Ballot	12/3/2019	12/12/2019	Quorum: 88.76%/89.02%/89.02 %/88.98%/89.96%/89. 06%/88.72%/87.89% Approval: 99.69%/99.36%/99.69 %/99.69%/99.59%/99. 38%/99.69%/99.68%	Affirmative--12/12/19		
622	Project 2018-04	Project 2018-04 Modifications to PRC-024-2	Final Ballot	12/4/2019	12/13/2019	Quorum: 89.26% Approval: 82.47%	Affirmative--11/4/19		
623	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Additional Ballot	11/1/2019	12/16/2019	Quorum: 81.89% Approval: 95.98%	Affirmative--12/12/19		
624	Technical Rationale for Reliability Standards	Technical Rationale for Reliability Standards	Non-binding Poll	12/9/2019	12/18/2019	Quorum: 85.46%/82.52%/82.83 %/82.35%/82.76%/86. 55%/81.77%/86.82%/ 82.76% Approval: 84.91%/88.89%/85.12 %/86.57%/86.57%/86. 79%/89.55%/88.75%/ 77.78%	Affirmative--12/12/19		
625	Project 2017-07	Project 2017-07 Standards Alignment with Registration	Final Ballot	1/14/2020	1/23/2020	Quorum: 89.53%/89.8%/89.8%/ 89.76%/90.83%/89.84 %/89.88%/88.67% Approval: 99.69%/99.69%/99.69 %/99.69%/99.6%/99.3 8%/99.69%/99.69%	Affirmative--12/12/19		
626	Project 2019-02	Project 2019-02 BES Cyber System Information Access Management	Initial Ballot	1/24/2020	2/3/2020	Quorum: 92.09%/92.78%/91.58 % Approval: 15.37%/13.04%/22.30 %	Abstain--1/31/20		
627	Project 2019-03	Project 2019-03 Cyber Security Supply Chain Risks	Initial Ballot	1/27/2020	3/11/2020	Quorum: 88.37% Approval: 50.51%	Abstain--2/26/20		
628	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Final Ballot	3/26/2020	4/6/2020	Quorum: 87.92% Approval: 96.28%	Affirmative--12/12/19		

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
629	Technical Rationale for Reliability Standards	Technical Rationale for Reliability Standards	Non-binding Poll	4/10/2020	4/20/2020	Quorum: 81.93%/82.24%/80.49 %/82.17%/81.44%/81. 78%/81.3%/81.92%/8 0.93%/81.73% Approval: 86.475/87.77%/87.12 %/85.48%/85.7%/87.1 %/86.93%/85.8%/76.9 %/79.25%	Affirmative--4/17/20		
630	Project 2019-03	Project 2019-03 Cyber Security Supply Chain Risks	Additional Ballot	6/12/2020	6/22/2020	Quorum: 78.74% Approval: 34.44%	Abstain--2/26/20		
631	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Initial/Additional Ballot	7/24/2020	8/26/2020	Quorum: 81.48%/81.73%/81.35 %/81.15%/80.57%/80. 98%/80.43%/80.67%/ 91.18%/91.48% Approval: 58.50%/88.32%/79.26 %/86.98%/72.82%/88. 78%/88.50%/89.16%/ 85.21%/81.17%	Affirmative--7/24/20		
632	Project 2019-02	Project 2019-02 BES Cyber System Information Access Management	Additional Ballot	9/11/2020	9/21/2020	Quorum: 84.98%/83.82%/82.84 % Approval: 32.80%/23.06%/50.49 %	Abstain--9/17/20		
633	Project 2019-03	Project 2019-03 Cyber Security Supply Chain Risks	Final Ballot	10/7/2020	10/16/2020	Quorum: 83.56% Approval: 76.76%	Abstain--2/26/20		
634	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Additional Ballot	11/27/2020	12/7/2020	Quorum: 82.82%/82.41% Approval: 66.61%/89.79%	Affirmative--12/4/20		
635	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Initial Ballot	4/3/2019	4/12/2019	Quorum: 89.93%/86.61% Approval: 95.91%/100%	Affirmative--1/4/21		
636	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Final Ballot	1/19/2021	1/28//21	Quorum: 91.04% Approval: 95.96%	Affirmative--1/4/21		

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

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

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

RSC Meeting #21-1, Agenda Item 4.3: Comment History
(As of 2/5/2021)

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 #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

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	<u>Yes 4/4/11</u>
14.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		3/9/11	4/8/11	<u>Yes 4/8/11</u>
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	<u>Yes 4/15/11</u>
17.	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3 - CIP-005	CIP-005		3/29/11	4/28/11	<u>Yes 4/27/11</u>
18.	Project 2009-06	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	FAC-008-3		3/17/11	5/2/11	<u>Yes 5/2/11</u>
19.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		4/13/11	5/12/11	<u>Yes 5/9/11</u>
20.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		4/28/11	5/27/11	<u>Yes 5/27/11</u>
21.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	TPL-001-2		4/18/11	5/31/11	<u>Yes 5/31/11</u>
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	<u>Yes 6/9/11</u>
23.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		5/11/11	6/10/11	<u>Yes 6/10/11</u>
24.	NERC RoP	Rules of Procedure Development Team: BES Definition Exception Process	BES Definition Exception Process		5/11/11	6/10/11	<u>Yes 6/10/11</u>

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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	
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
35..	N/A	CAN-0016 CIP-001 R1 - Sabotage Reporting Procedure	CAN-0016 CIP-001, R1		8/15/11	9/6/11	<u>Yes 9/6/11</u>
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	
37.	NERC RSDP	NERC 2012-2014 Reliability Standards Development Plan	2012-2014 RSDP		9/12/11	9/26/11	<u>Yes 9/26/11</u>
38.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		8/15/11	9/28/11	<u>Yes 9/28/11</u>
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	<u>Yes 10/10/11</u>
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	<u>Yes 10/10/11</u>
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	<u>Yes 10/14/11</u>
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	<u>Yes 10/27/11</u>
44.	N/A	CAN-0010--Definition of "Annual" and Implementation of Annual Requirements	CAN-0010 Definition of Annual		10/10/11	10/31/11	<u>Yes 10/31/11</u>

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
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	

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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	
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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	
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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	<u>Yes 6/20/12</u>
90.	N/A	Adequate Level of Reliability Revised Definition and Associated Documents	Adequate Level of Reliability (ALR)		4/25/12	6/25/12	<u>Yes 6/25/12</u>
91.	N/A	Order 754 - Request for Data or Information	Data Request		5/11/12	6/25/12	<u>Yes 6/25/12</u>
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	<u>Yes 6/27/12</u>
93.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		5/29/12	6/27/12	<u>Yes 6/27/12</u>
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	<u>Yes 7/3/12</u>
			BAL-002-2		6/4/12	7/3/12	<u>Yes 7/3/12</u>
			BAL-012-1		6/4/12	7/3/12	<u>Yes 7/3/12</u>
			BAL-013-1		6/4/12	7/3/12	<u>Yes 7/3/12</u>
95.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		5/21/12	7/5/12	<u>Yes 7/5/12</u>
96.	N/A	Cost Effective Analysis Process (CEAP) for NERC ERO Standards	CEAP		5/7/12	7/6/12	<u>Yes 7/6/12</u>
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	<u>Yes 7/6/12</u>
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	<u>Yes 7/9/12</u>

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
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	

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
			RSAP		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	
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	

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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 #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

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 5/6/13
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 #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

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	<u>Yes 8/23/13</u>
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	<u>Yes 8/23/13</u>
165.	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	MOD-001-2	Formal	7/11/13	8/26/13	<u>Yes 8/26/13</u>
166.	Project 2010-01	Project 2010-01 - Training - PER-005-2	PER-005-2	Formal	7/19/13	9/03/13	<u>Yes 9/3/13</u>
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	<u>Yes 9/3/13</u>
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	<u>Yes 9/4/13</u>
169.	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	7/22/13	9/04/13	<u>Yes 9/4/13</u>
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	<u>Yes 9/4/13</u>
171	Project 2012-13	Project 2012-13 - NUC Five-Year Review	NUC-001-2	5-year review	7/26/13	9/9/13	<u>Yes 9/9/13</u>
172	2014-2016 RSDP	2014-2016 Reliability Standards Development Plan	Reliability Standards Development Plan	Annual Review	8/30/13	9/13/13	<u>Yes 9/13/13</u>
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	<u>Yes 9/16/13</u>
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	<u>Yes 9/16/13</u>

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
188	Project 2009-03	Project 2009-03 Emergency Operations	SAR	Informal	11/06/13	12/05/13	<u>Yes 12/5/13</u>
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	<u>Yes 12/11/13</u>
190	Project 2007-11	Project 2007-11 - Disturbance Monitoring	PRC-002-2	Formal	11/01/13	12/16/13	<u>Yes 12/16/13</u>
191	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-027	Formal	11/04/13	12/18/13	<u>Yes 12/18/13</u>
192	Project 2014-01	Project 2014-01 - Standards Applicability for Dispersed Generation Resources	SAR	Formal	11/20/13	12/19/13	<u>Yes 12/19/13</u>
193	Project 2010-01	Project 2010-01 Training - PER-005-2	PER-005-2	Formal	12/4/13	1/22/14	<u>Yes 1/17/14</u>
194	Project 2010-03	Project 2010-03 Modeling Date - MOD B	MOD-033-1	Formal	12/6/13	1/22/14	<u>Yes 1/21/14</u>
195	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	INT-004-3 INT-010-2	Formal	1/10/14	1/24/14	<u>Yes 1/22/14</u>
196	Project 2007-02	Project 2007-02 Operating Personnel	COM-002-4	Formal	1/22/14	1/31/14	<u>Yes 1/31/14</u>
197	Project 2014-02	Project 2014-02 Standard Authorization Request – Cyber Security Standards	CIP SAR	Informal	1/17/14	2/18/14	<u>Yes 2/18/14</u>
198	2014 Work Plan	2014 Work Plan for NERC Reliability Standards Development	2014 Work plan			2/21/13	<u>Yes 2/21/14</u>
199	Project 2010-17	Project 2010-17 Definition of Bulk Electric System - Phase 2	BES	Informal	1/29/14	2/27/14	<u>Yes 2/27/14</u>
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	<u>Yes 3/2/14</u>

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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
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	CIP-002 to CIP-011	Formal	06/02/14	07/17/14	Yes 7/16/14

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		– Cyber Security Standards					
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 for BAL-005 and BAL-006	BAL-005 BAL-006	Informal	07/16/14	08/14/14	Yes 8/12/14
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-	TOP-001-3 TOP-002-4	Formal	08/6/14	09/19/14	Yes 9/22/14

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		IRO Reliability Standards	TOP-003-3 IRO-001-4 IRO-002-4 IRO-008-2 IRO-010-2 IRO-014-3 IRO-017-1				
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 CIP-007-X CIP-010-X CIP-011-X	Formal	09/03/14	10/17/14	Yes 10/17/14
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

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
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	Project 2014-01	Project 2014-01 – Standards Applicability for Dispersed Generation Resources	PRC-001-1.1 PRC-019-2 PRC-024-1	Formal	11/05/14	12/23/14	Yes 12/22/14
251	Project 2014-03	Project 2014-03 Revisions to TOP/IRO Reliability Standards TOP-001-3	TOP-001-3	Formal	12/29/14	1/7/15	Yes 1/6/15
252	Project 2014-02	Project 2014-02 CIP Version 5 Revisions	CIP-003-7 CIP-004-7 CIP-007-7 CIP-010-3 CIP-011-3 CIP-003-7 CIP-010-3 Implementation Plan	Formal	12/30/14	1/9/15	Yes 1/9/15
253	Project 2014-04	Project 2014-04 Physical Security SAR	SAR	Informal	12/15/14	1/13/15	Yes 1/12/15
254	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	White Paper Appendix A Appendix B	Informal	12/22/14	1/20/15	Yes 1/20/15
255	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed	PRC-005-5	Informal	12/22/14	1/20/15	Yes 1/22/15

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Generation Resources					
257	Project 2010-14.1	Project 2010-14.1 Balancing Authority Reliability-based Control	BAL-002-2	Formal	1/29/15	3/18/15	Yes 3/16/15
258	Reliability Guideline	Reliability Guideline: Loss of Real-Time Reliability Tools Capability/Loss of Equipment Significantly Affecting ICCP Data		Formal	2/19/15	4/6/15	Yes 4/6/15
259	Project 2008-02.2	Project 2008-02.2 Phase 2 UVLS: Misoperation	PRC-010-2	Formal	2/20/15	4/7/15	Yes 4/7/15
260	Project 2014-04	Project 2014-04 Physical Security	CIP-014-2	Formal	2/20/15	4/9/15	Yes 4/9/15
261	Project 2015-04	Project 2015-04 Alignment of Terms	SAR	Formal	2/24/15	4/13/15	Yes 4/13/15
262	Project 2007-17.4	Project 2007-17.4 PRC-005 Order No. 803 Directives	SAR	Informal	3/12/15	4/10/15	Yes 4/13/15
263	Project 2015-06	Project 2015-06 Interconnection Reliability Operations and Coordination	SAR	Informal	3/16/15	4/15/15	Yes 4/15/15
264	Project 2010-14.2.2	Project 2010-14.2.2 Phase 2 of Balancing Authority Reliability-based Controls: Time Error Correction	SAR	Informal	3/17/15	4/15/15	Yes 4/15/15
265	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-008-1	Informal	3/27/15	5/11/15	Yes 5/11/15
266	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-006-2	Informal	3/27/15	5/11/15	Yes 5/11/15
267	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-005-2	Informal	3/27/15	5/11/15	Yes 5/11/15
268	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-004-2	Informal	3/27/15	5/11/15	Yes 5/11/15

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
269	Project 2007-06	Project 2007-06 System Protection Coordination PRC-027-1 (Draft 5)	PRC-027-1	Formal	4/1/15	5/15/15	Yes 5/15/15
270	Project 2010-04.1	Project 2010-04.1 MOD-031 FERC Order No. 804 Directives	SAR	Informal	4/16/15	5/19/15	Yes 5/19/15
271	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems – RAS	PRC-012-2	Informal	4/30/15	5/20/15	Yes 5/20/15
272	Project 2015-03	Project 2015-03 Periodic Review of System Operating Limit Standards	FAC-010-3 FAC-011-3 FAC-014-2	Formal	5/4/15	6/17/15	Yes 6/17/15
273	Project 2015-06	Project 2015-06 Interconnection Reliability Operations and Coordination	IRO-006-East-2 IRO-009-2	Formal	5/21/15	7/8/15	Yes 7/8/15
274	Project 2007-17.4	Project 2007-17.4 PRC-005 FERC Order No. 803 Directive	PRC-005-3	Formal	6/11/15	7/10/15	Yes 7/10/15
275	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generations Resources	PRC-004-2.1 PRC-005-2 PRC-005-3	Informal	6/12/15	7/13/15	Yes 7/13/15
276	Project 2015-07	Project 2015-07 Internal Communications Capabilities	COM-001-2	Informal	6/11/15	7/15/15	Yes 7/15/15
277	Project 2015-04	Alignment of Terms	Glossary Terms	Formal	6/12/15	7/23/15	Yes 7/23/15
278	Project 2009-02	Real-time Monitoring and Analysis Capabilities	SAR	Formal	7/16/15	8/17/15	Yes 8/17/15
279	NERC 2016-2018	Reliability Standards Development Plan	Development Plan	Formal	7/16/15	8/17/15	Yes 8/17/15
280	Project 2015-08	Emergency Operations	EOP-004-2 EOP-005-2 EOP-006-2 EOP-008-1	Informal	7/21/15	8/19/15	Yes 8/19/15
281	Project 2010-14.1	Phase 1 of Balancing Authority Reliability-based Controls	BAL-002-2	Formal	7/7/15	8/20/15	Yes 8/20/15
282	Project 2010-	Phase 2 of Balancing Authority	BAL-004-0	Survey	8/12/15	8/25/15	Yes 8/25/15

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
	14.2.2	Reliability-based Controls: Time Error Correction					
283	Project 2007-06.2	Phase 2 of System Protection Coordination	TOP-009-1	Formal	7/29/15	9/11/15	Yes 9/11/15
284	Project 2007-06	System Protection Coordination	PRC-027-1	Formal	7/29/15	9/11/15	Yes 9/11/15
285	Project 2010-14.2.1	Phase 2 of Balancing Authority Reliability-based Controls	BAL-005-1 BAL-006-3	Formal	7/30/15	9/14/15	Yes 9/14/15
286	Project 2007-17.4	PRC-005 FERC Order No. 803 Directive	PRC-005-6	Formal	7/30/15	9/16/15	Yes 9/16/15
287	Project 2010-04.1	MOD-031 FERC Order No. 804 Directives	MOD-031-2	Formal	7/31/15	9/18/15	Yes 9/18/15
288	Project 2015-09	Establish and Communicate System Operating Limits	FAC-010-3 FAC-011-3 FAC-014-2	Informal	8/20/15	9/21/15	Yes 9/21/15
289	Project 2010-07.1	Vegetation Management	FAC-003-3	Informal	8/24/15	9/28/15	Yes 9/28/15
290	Project 2010-05.3	Phase 3 of Protection Systems: Remedial Action Schemes	PRC-012-2	Formal	8/20/15	10/5/15	Yes 10/5/15
291	Project 2009-02	Real-time Reliability Monitoring and Analysis Capabilities	IRO-018-1 TOP-010-1	Formal	9/24/15	11/9/15	Yes 11/9/15
292	Project 2010-14.2.2	Phase 2 of Balancing Authority Reliability-based Controls	BAL-004-0	Formal	9/24/15	11/12/15	Yes 11/12/15
293	Project 2015-07	Internal Communications Capabilities	COM-001-3	Formal	9/25/15	11/16/15	Yes 11/16/15
294	Project 2007-06.2	Phase 2 of System Protection Coordination	TOP-009-1	Formal	10/6/15	11/19/15	Yes 11/19/15
295	Project 2010-07.1	Vegetation Management	FAC-003-3	Formal	10/30/15	12/16/15	Yes 12/16/15
296	Project 2015-10	Single Points of Failure SAR	TPL-001	Informal	11/12/15	12/17/15	Yes 12/17/15
297	Project 2010-05.3	Phase 3 of Protection Systems RAS	PRC-012-2	Formal	11/25/15	1/8/16	Yes 1/8/16
298	Project 2010-14.2.1	Phase 2 of Balancing Authority Reliability-based Controls	BAL-005-1 FAC-001-3 BAL-006-2	Formal	12/31/15	1/11/16	Yes 1/11/16

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
299	Project 2009-02	Real-time Reliability Monitoring and Analysis Capabilities	IRO-018-1 TOP-010-1	Formal	12/10/15	1/25/16	Yes 1/25/16
300	Project 2016-01	Modifications to TOP and IRO Standards	SAR	Informal	1/22/16	2/22/16	Yes 2/22/16
301	Project 2010-05.3	Phase 3 of Protection Systems RAS	PRC-012-2	Formal	2/3/16	3/18/16	Yes 3/18/16
302	Project 2016-02	Modifications to CIP Standards	SAR	Informal	3/23/16	4/21/16	Yes 4/21/16
303	Project 2007-06.2	Phase 2 of System Protection Coordination	PER-006-1 & Two Definitions	Formal	3/10/16	4/25/16	Yes 4/25/16
304	Project 2015-07	Internal Communications Capabilities	COM-001-3	Formal	3/23/16	5/9/16	Yes 5/6/16
305	CEP	Cost Effectiveness Pilot	TPL-001-4	Informal	4/27/16	5/26/16	Yes 5/26/16
306	Project 2013-03	Geomagnetic Disturbance Mitigation Revised White Papers	SAR	Informal	5/12/16	6/13/16	Yes 6/13/16
307	Project 2015-10	Single Points of Failure	SAR	Informal	5/26/16	6/24/16	Yes 6/24/16
308	Project 2016-02	Modifications to CIP Standards	SAR	Informal	6/1/16	6/30/16	Yes 6/30/16
309	Draft 2017-2019	Reliability Standards Development Plan	RSDP	Informal	6/20/16	7/19/16	Yes 7/19/16
310	EPR	Enhanced Periodic Review Standing Review Team	Standards Grading	Informal	6/30/16	8/1/16	Yes 8/1/16
311	Project 2016-01	Modifications to TOP and IRO Standards	IRO-002-5 TOP-001-4	Formal	6/20/16	8/3/16	Yes 8/3/16
312	Project 2015-09	Establish and Communicate System Operating Limits	FAC-014-3	Formal	7/14/16	8/12/16	Yes 8/12/16
313	Project 2015-09	Establish and Communicate System Operating Limits	FAC-011-4	Formal	7/14/16	8/12/16	Yes 8/12/16
314	Project 2015-08	Emergency Operations	EOP-005-3 EOP-006-3 EOP-008-2	Formal	6/30/16	8/15/16	Yes 8/15/16
315	Project 2016-02	Modifications to CIP Standards	CIP-003-7	Formal	7/21/16	9/6/16	Yes 9/6/16
316	FMAG	Functional Model Advisory Group	Reliability Functional Model and Technical Document	Informal	7/21/16	9/7/16	Yes 9/7/16
317	Project	Emergency	EOP-004-4	Formal	7/25/16	9/8/16	Yes 9/8/16

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
	2015-08	Operations					
318	Project 2015-INT-01	Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)	CIP-002-5.1	Formal	7/27/16	9/12/16	Yes 9/12/16
319	Project 2016-01	Modifications to TOP and IRO Standards SAR	TOP-001-3 IRO-002-4	Formal	8/31/16	10/17/16	Yes 10/14/16
320	Project 2016-04	Modifications to PRC-025-1 SAR	PRC-025-1	Formal	9/16/16	10/18/16	Yes 10/18/16
321	Project 2016-03	Cyber Security Supply Chain Management	SAR	Informal	10/20/16	11/18/16	Yes 11/18/16
322	Project 2016-02	Modifications of CIP Standards	CIP-003-TCA	Informal	11/1/16	11/18/16	Yes 11/18/16
323	Project 2016-02	Modifications of CIP Standards	CIP-003-7	Formal	11/23/16	12/5/16	Yes 12/5/16
324	Project 2015-08	Emergency Operations	EOP-005-3 EOP-006-3	Formal	10/26/16	12/9/16	Yes 12/9/16
325	Project 2015-08	Emergency Operations	EOP-004-4	Formal	11/18/16	1/6/17	Yes 1/6/17
326	Project 2013-03	Geomagnetic Disturbance Mitigation	SAR	Informal	12/16/16	1/20/17	Yes 1/20/17
327	Project 2016-02	Modifications of CIP Standards	CIP-003-7(i)	Formal	12/12/16	1/25/17	Yes 1/25/17
328	Project 2016-EPR-01	Enhanced Periodic Review of Personnel Performance, Training and Qualifications Standard (PER)	PER-001-0.2 PER-003-1 PER-004-2	Formal	1/10/17	2/23/17	Yes 2/23/17
329	Project 2016-03	Cyber Security Supply Chain Risk Management	CIP-013-1	Formal	1/19/17	3/6/17	Yes 3/6/17
330	Project 2016-04	Modifications to PRC-025-1	SAR	Informal	3/20/17	4/3/17	Yes 4/3/17
331	Project 2016-02	Modifications to CIP Standard	Virtualization	Informal	3/14/17	4/11/17	Yes 4/11/17
332	Project 2016-02	Modifications to CIP Standard	TOCC	Informal	3/14/17	4/11/17	Yes 4/11/17
333	Project 2016-EPR-02	Enhanced Periodic Review of Voltage and Reactive (VAR) Standards	VAR-001-4.1	Formal	2/28/17	4/13/17	Yes 4/13/17
334	Project 2016-EPR-02	Enhanced Periodic Review of Voltage and Reactive (VAR) Standards	VAR-002-4	Formal	2/28/17	4/13/17	Yes 4/13/17
335	SPM	Revisions to the NERC Standard	SPM	Formal	3/20/17	5/3/17	Yes 5/3/17

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Processes Manual					
336	Project 2015-10	Single Points of Failure	TPL-001-5	Informal	4/25/17	5/24/17	Yes 5/24/17
337	Project 2016-03	Cyber Security Supply Chain Risk Management	CIP-005-6 CIP-010-3 CIP-013-1	Formal	5/2/17	6/15/17	Yes 6/15/17
338	Project 2017-01	Modifications to BAL-003-1.1 SAR	BAL-003-1.1	Formal	6/19/17	7/18/17	Yes 7/18/17
339	Project 2017-06	Modifications to BAL-002-2 SAR	BAL-002-2	Informal	6/20/17	7/20/17	Yes 7/20/17
340	Project 2017-02	Modifications to Personnel Performance, Training and Qualifications Standards	PER-003-1 PER-004-2	Informal	6/21/17	7/24/17	Yes 7/24/17
341	2018-2010	Reliability Standards Development Plan		Formal	6/22/17	7/25/17	Yes 7/26/17
342	Standards Grading	Periodic Review Standing Review Team	Standards Grading	Informal	6/19/17	8/2/17	Yes 8/2/17
343	Project 2013-03	Geomagnetic Disturbance Mitigation	TPL-007-2	Formal	6/28/17	8/11/17	Yes 8/11/17
344	Project 2017-07	Alignment with Registration	Registration	Formal	8/1/17	8/30/17	Yes 8/30/17
345	Project 2017-07	Alignment with Registration	MOD-032-1 SAR	Formal	8/1/17	8/30/17	Yes 8/30/17
346	Reliability Guideline	Area Control Error Diversity Interchange Process	ACE Process	Formal	7/18/17	8/31/17	Yes 8/31/17
347	Project 2016-04	Modifications to PRC-025-1	PRC-025-2	Formal	7/25/17	9/7/17	Yes 9/7/17
348	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	7/27/17	9/11/17	Yes 9/11/17
349	Project 2016-02	Modifications to CIP Standard	Technical Rationale and Justification for CIP-012-1	Informal	8/14/17	9/12/17	Yes 9/12/17
350	Project 2016-02	Modifications to CIP Standard	Definition of Control Center	Informal	8/14/17	9/12/17	Yes 9/12/17
351	Project 2015-10	Single Points of Failure	TPL-001-5	Formal	9/8/17	10/23/17	Yes 10/23/17
352	Project 2016-02	Modifications to CIP Standard	CIP-002-6	Formal	9/14/17	10/30/17	Yes 10/30/17
353	Project 2015-09	Establish and Communicate System Operating Limits	Proposed Definitions of System Operating Limit (SOL) and SOL Exceedance	Informal	9/29/17	10/30/17	Yes 10/30/17
354	Project 2016-02	Modifications to CIP Standard	Virtualization	Informal	10/6/17	11/2/17	Yes 11/2/17
355	Project 2015-09	Establish and Communicate System Operating	FAC-010 FAC-011 FAC-014	Formal	9/29/17	11/13/17	Yes 11/13/17

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Limits					
356	Project 2017-01	Modifications to BAL-003-1.1	SAR	Formal	11/2/17	12/1/17	Yes 12/1/17
357	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	10/27/17	12/11/17	Yes 12/11/17
358	Project 2016-02	Modifications to CIP Standard	Technical Rationale/Justification	Informal	11/20/17	12/11/17	Yes 12/11/17
359	Project 2017-03	FAC-008-3 Periodic Review	FAC-008-3	Formal	10/30/17	12/13/17	Yes 12/13/17
360	Project 2016-04	Modifications to PRC-025-1	PRC-025-1	Formal	10/30/17	12/13/17	Yes 12/13/17
361	Project 2017-07	Alignment with Registration	SAR	Formal	12/11/17	1/9/18	Yes 1/9/18
362	Project 2017-05	NUC-001-3	NUC-001-3	Formal	12/15/17	1/29/18	Yes 1/29/18
363	Project 2017-04	INT Periodic Review	INT-004-3.1 INT-006-4 INT-009-2.1 INT-010-2.1	Formal	1/10/18	2/23/18	Yes 2/23/18
364	Project 2017-07	Standards Alignment with Registration	Multiple Standards	Formal	2/1/18	3/2/18	Yes 3/2/18
365	Project 2017-02	Modifications to Personnel Performance, Training and Qualifications (PER) Standards	PER-003-1 PER-004-2	Formal	1/22/18	3/7/18	Yes 3/7/18
366	Project 2015-10	Single Points of Failure	TPL-001-5	Formal	2/23/18	4/23/18	Yes 4/23/18
367	Project 2018-01	Canadian-specific Revisions to TPL-007-2 SAR	TPL-007-2 SAR	Formal	3/30/18	4/30/18	Yes 4/30/18
368	Project 2016-02	Modifications to CIP Standard	CIP-002-6	Formal	3/16/18	4/30/18	Yes 4/30/18
369	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	3/16/18	4/30/18	Yes 4/30/18
370	Project 2016-02	Modifications to CIP Standard	Control Center Definition and Implementation	Formal	3/16/18	4/30/18	Yes 4/30/18
371	Standards Grading	2018 Periodic Review Standing Review Team	Standard Grading	Informal	5/14/18	6/28/18	Yes 6/28/18
372	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	5/18/18	7/3/18	Yes 7/2/18
373	SER	Standard Efficiency Review	SAR	Informal	6/7/18	7/10/18	Yes 7/10/18
374	Project 2016-02	Modifications to CIP Standard	CIP-002-5.1a SAR	Informal	6/14/18	7/13/18	Yes 7/13/18
375	Project 2016-02	Modifications to CIP Standard	CIP-003-7 SAR Order 843	Informal	6/14/18	7/13/18	Yes 7/13/18
376	SPM	Standards Processes Manual	SPM	Formal	6/25/18	8/9/18	Yes 8/9/18

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
377	Project 2018-01	Canadian-specific Revisions to TPL-007-2	TPL-007-2	Informal	8/10/18	9/6/18	Yes 9/6/18
378	Project 2018-02	Modifications to CIP-008 Cyber Security Incident Reporting SAR	CIP-008-5	Informal	8/10/18	9/10/18	Yes 9/10/18
379	Project 2015-10	Single Points of Failure	TPL-001-5	Formal	7/30/18	9/14/18	Yes 9/14/18
380	Functional Model Advisory Group	Functional Model Advisory Group	Functional Model Advisory Group	Informal	8/3/18	9/19/18	Yes 9/17/18
381	Project 2017-01	Modifications to BAL-003-1.1	BAL-003-1.1	Informal	9/6/18	9/20/18	Yes 9/20/18
382	SER	Standard Efficiency Review	SAR	Formal	8/28/18	9/26/18	Yes 9/26/18
383	Project 2016-02	Modifications to CIP Standards	CIP-002-6	Formal	8/23/18	10/9/18	Yes 10/9/18
384	Project 2016-02	Modifications to CIP Standards	CIP-003-8	Formal	8/23/18	10/9/18	Yes 10/9/18
385	Project 2015-09	Establish and Communicate System Operating Limits	FAC-010 FAC-011 FAC-014	Formal	8/24/18	10/17/18	Yes 10/17/18
386	Project 2018-02	Cyber Security – Incident Reporting and Response Planning	CIP-008-6	Formal	10/3/18	10/22/18	Yes 10/22/18
387	Project 2018-01	Canadian-specific Revisions to TPL-007-2	TPL-007-2	Formal	10/2/18	11/15/18	Yes 11/15/18
388	Project 2018-02	Cyber Security – Incident Reporting and Response Planning	CIP-008-6	Formal	11/15/18	11/29/18	Yes 11/29/18
389	Project 2016-02	Modifications to CIP Standards	Virtualization	Informal	11/2/18	12/18/18	Yes 12/18/18
390	Project 2017-01	Modifications to BAL-003-1.1	BAL-003-1.1	Formal	12/4/18	1/17/19	Yes 1/17/19
391	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Formal	12/19/18	1/18/19	Yes 1/18/19
392	Standard Efficiency Review	Standard Efficiency Review	SER Phase 2 Concepts Survey	Informal	2/22/19	3/22/19	Yes 3/22/19
393	Project 2019-01	Modifications to TPL-007-3	TPL-007-3	Informal	2/25/19	3/26/19	Yes 3/26/19
394	Project 2018-03	Standard Efficiency Review Retirements	FAC-008-4 INT-006-5 INT-009-3 IRO-002-6 PRC-004-6 TOP-001-5	Formal	2/27/19	4/12/19	Yes 4/12/19

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
			VAR-001-6 FAC-013-2 INT-004-3.1 INT-010-2.1 MOD-001-1a MOD-004-1 MOD-008-1 MOD-020-0 MOD-028-2 MOD-029-2a MOD-030-3 MOD-001-2				
395	Project 2019-02	BES Cyber System Information Access Management	CIP-004-6	Formal	3/28/19	4/26/19	Yes 4/26/19
396	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Formal	4/17/19	5/31/19	Yes 5/31/19
397	Project 2016-02	Modifications to CIP Standards	Virtualization White Paper	Informal	5/30/19	6/28/19	Yes 6/28/19
398	Project 2016-02	Modifications to CIP Standards	CIP-002-6	Formal	6/3/19	7/17/19	Yes 7/17/19
399	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Informal	6/27/19	7/26/19	Yes 7/26/19
400	Project 2019-03	Cyber Security Supply Chain Risks	CIP-005-6 CIP-010-3 CIP-013-1	Informal	7/2/19	8/1/19	Yes 8/1/19
401	SER	CIP SER	CIP Standards	Formal	7/3/19	8/26/19	Yes 8/26/19
402	Project 2019-04	Modifications to PRC-005-6	PRC-005-6 SAR	Formal	7/30/19	8/28/19	Yes 8/28/19
403	Project 2019-05	Modifications to PER-003-2	PER-003-2	Informal	8/1/19	8/30/19	Yes 8/30/19
404	Project 2016-02	Modifications to CIP Standards	CIP-005	Informal	8/9/19	9/26/19	Yes 9/26/19
405	EMP	Electromagnetic Pulses Task Force Draft Strategic Recommendation	EMP	Informal	8/30/19	9/30/19	Yes 9/30/19
406	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Formal	9/20/19	11/4/19	Yes 11/4/19
407	Project 2019-06	Cold Weather SAR	SAR	Formal	10/4/19	11/5/19	Yes 11/5/19
408	Project 201707	Standards Alignment with Registration	FAC-002-3 IRO-010-3 MOD-031-3 MOD-033-2 NUC-001-4 PRC-006-4 TOP-003-4	Formal	10/29/19	12/12/19	Yes 12/12/19
409	Project 2016-02	Modifications to CIP Standards	CIP-002-6	Formal	11/1/19	12/16/19	Yes 12/16/19
410	Project	Technical Rationale for Reliability	IRO-001-4 IRO-002-6	Informal	11/4/19	12/18/19	Yes 12/18/19

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Standards	IRO-006-East-2 IRO-008-2 IRO-009-2 IRO-010-2 IRO-014-3 IRO-017-1 IRO-018-1(i)				
411	Project 2019-02	BES Cyber System Information Access Management	CIP-004-6	Formal	12/20/19	2/3/20	Yes and No 2/3/20
412	Project 2019-03	Cyber Security Supply Chain Risks	CIP-005-6 CIP-010-3 CIP-013-1	Formal	1/27/20	3/11/20	Yes and No 3/11/20
413	Project 2019-06	Cold Weather SAR	SAR	Formal	2/19/20	3/19/20	Yes 3/19/20
414	Project	Technical Rationale for Reliability Standards	IRO-001-4 IRO-002-6 IRO-006-East-2 IRO-008-2 IRO-009-2 IRO-010-2 IRO-014-3 IRO-017-1 IRO-018-1(i)	Informal	4/10/20	4/20/20	Yes 4/20/20
415	Project 2020-01	Modifications to MOD-032-1	MOD-032-1	Informal	3/24/20	4/24/20	Yes 4/24/20
416	Project 2020-02	Transmission-connected Resources SAR	MOD-025 MOD-026 MOD-027 PRC-019 PRC-024	Informal	3/30/20	5/13/20	Yes 5/13/20
417	Project 2019-06	Cold Weather SAR	SAR	Informal	4/22/20	5/21/20	Yes 5/21/20
418	SER	Operational Data Exchange Simplification SAR	SAR	Survey	3/12/20	5/27/20	Yes 5/28/20
419	Project 2020-03	Supply Chain Low Impact Revisions	SAR	Informal	4/3/20	6/3/20	Yes 6/3/20
420	Project 2020-04	Modifications to CIP-012	SAR	Informal	4/8/20	6/11/20	Yes 6/11/20
421	Project 2019-03	Cyber Security Supply Chain Risks	CIP-005-6 CIP-010-3 CIP-013-1	Formal	5/7/20	6/22/20	Yes 6/22/20
422	Project 2019-04	Modifications to PRC-005-6	PRC-005-6	Formal	6/2/20	7/8/20	Yes 7/8/20
423	Project 2015-09	Establish and Communicate System Operating Limits	CIP-014-3 FAC-003-5 FAC-011-4 FAC-013-3 FAC-014-3 PRC-002-3 PRC-026-2 TOP-001-6	Formal	6/19/20	8/3/20	Yes 8/3/20

RSC Meeting #21-1, Agenda Item 4.3: Comment History

(As of 2/5/2021)

[illegible]

Note: RSC past comment forms are posted on the NPCC Website under “[Standards - Regional Standards Comments](#).”

2/3/2021

Type	Document	Description	Comments	Status

NPCC Directory Executive Tracking Summary

Revised: 2/3/2021

	Document	Title	Responsible Task Force	Latest Version	Comments	Status
Directories						
	Directory #1	Design and Operation of the Bulk Power System	TFCP	Oct-15	TFCP/TFCO currently developing draft scope 2021 Directory #1 periodic review.	
	Directory #2	Emergency Operations	TFCO	Jun-18		Revisions approved by Full Member Committee June 29, 2018.
	Directory #3	Maintenance Criteria for Bulk Power System Protection	TFSP	Jun-09		Directory#3 retired effective April 1st, 2015 coinciding with the enforcement date of PRC -005-2.
	Directory #4	Bulk Power System Protection Criteria	TFSP	Sep-15		Revisions approved by Full Member Committee January 30, 2020.
	Directory #5	Reserve	TFCO	Oct-12		Revisions approved by Full Member Committee September 27, 2019.
	Directory #6	Regional Reserve Sharing	TFCO	Apr-12		Revisions approved by Full Member Committee September 27, 2019.
	Directory #7	Remedial Action Schemes	TFSP	Dec-20		Revisions approved by Full Member Committee December 22, 2020
	Directory #8	System Restoration	TFCO	Sep-18		Revisions Approved by Full Member Committee September 25, 2018
	Directory #9	Verification of Generator Gross and Net Real Power Capability	TFCO	Dec-11		NPCC Full Member Committee approved retirement of D#9 and D#10 upon full enforcement of MOD-25-2. (July 1, 2019).
	Directory #10	Verification of Generator Gross and Net Reactive Power Capability	TFCO	Dec-11		See D#9.
	Directory#11	Disturbance Monitoring	TFSP	Oct-16	TFSP has begun its periodic review in November 2020.	Pending 1st Open Process Posting.
	Directory #12	Automatic UFLS	TFSS	Jul-13		TFSS to consider retirement upon full enforcement of PRC-006-NPCC-2.
Criteria						
	A-10	Classification of BPS Elements	TFCP	Dec-09		Revisions Approved by Full Member Committee January 27, 2020.
Procedures						

NPCC Directory Criteria Clarifications

Revised: **2/3/2021**

/ 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	3/4/2015	TFSP	Yes	Yes	Interpretation on behalf of IESO-MACD	Complete.
7	Directory#8 Clarification	System Restoration	12/1/2015	TFCO	Yes	Yes	Clarification on Behalf of OPG.	Complete.
8	Directory#5 Clarification	Reserve	9/7/2016	TFCO	Yes	Yes	Clarification on Behalf of the NYISO.	Complete
9	Directory#1 Clarification	Design and Operation of the BPS	9/7/2016	TFCP	Yes	Yes	Clarification on Behalf of New Brunswick	Complete
10	Directory#4 Clarification	System Protection Criteria	12/2/2016	TFSP	Yes	Yes	Clarification on Behalf of Eversource	Complete
11	Directory #4 Clarification	System Protection Criteria	12/5/2017	TFSP	Yes	Yes	Clarification on Behalf of Eversource.	Complete
12	Directory#1 Clarification	Design and Operation of the BPS	5/30/2018	TFCP/TFCO	Yes	Yes	Clarification on Behalf of NYSRC	Complete
13	Directory #8 Clarification	System Restoration	9/8/2020	TFCO	Yes	Yes	Clarification on Behalf of OPG.	Complete

2/3/2021

Filing Period	Filing Due	Filing Submitted	Comments
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.
January 1 to March 31, 2013	6/1/2013	N/A	No changes were made during the referenced period which required filing.
April 1 to June 30, 2013	9/1/2013	N/A	No changes were made during the referenced period which required filing.
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.
October 1 to December 31, 2013	3/1/2014	N/A	No changes were made during the referenced period which required filing.
January 1 to March 31, 2014	6/1/2014	N/A	No changes were made during the referenced period which required filing.
April 1 to June 30, 2014	9/1/2014	N/A	No changes were made during the referenced period which required filing.
July 1 to September 30, 2014	12/1/2014	N/A	No changes were made during the referenced period which required filing.
October 1 to December 31, 2014	3/1/2015	2/23/2015	(1) 10/15/14 NPCC Full Members approved retirement of D#3 effective 4/01/15 coinciding with enforcement date of PRC -005-2.
	3/1/2015	N/A	(2) 10/6/14 the RSC approved revisions to the Directory Manual which incorporated cost considerations into the Manual.
January 1st to March 31st 2015	6/1/2015	N/A	No changes were made during the referenced period which required filing.
April 1st to June 30th 2015	9/1/2015	N/A	No changes were made during the referenced period which required filing.
July 1 to September 30, 2015	12/1/2015	11/25/2015	Revisions to D#1 and D#4 approved by the Full Members on 9/30/2015.
October 1 to December 31, 2015	3/1/2016	N/A	No changes were made during the referenced period which required filing.
January 1st to March 31st, 2016	6/1/2016	N/A	No changes were made during the referenced period which required filing.
April 1 to June 30, 2016	9/1/2016	N/A	No changes were made during the referenced period which required filing.
July 1 to September 30, 2016	12/1/2016	N/A	No changes were made during the referenced period which required filing.
October 1 to December 31, 2016	3/1/2017	2/28/2017	Directory#11 approved by Full Members October 2016.
January 1st to March 31st 2017	6/1/2017	N/A	No changes were made during the referenced period which required filing.
April 1st to June 30th, 2017	9/1/2017	Will Not Be Filed.	Revisions to the A-01 Document approved by the Full Members on 4/21/2017.
July 1 to September 30, 2017	12/1/2017	2/28/2018	On August 3, 2017 NPCC Full Members approved retirement of Directories #9 and #10 effective July 1, 2019
October 1 to December 31, 2017	3/1/2018	2/28/2018	Revisions to D#8 approved by the Full Members on 10/06/2017.
January 1st to March 31st, 2018	6/1/2018	N/A	No changes were made during the referenced period which required filing.
April 1st to June 30th, 2018	9/1/2018	30-Aug-18	Revisions to Directory #2 approved by the Full Members on 6/29/2018.
July 1 to September 30, 2018	12/1/2018	26-Nov-18	Revisions to D#8 and Retirement of A-01 approved by the Full Members on 9/25/2018
October 1 to December 31, 2018	3/1/2019	N/A	No changes were made during the referenced period which required filing.

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: Quintin Lee
Program Manager - Reliability Compliance
Eversource Energy
780 North Commercial Street
Manchester, NH 03101
Office: (603) 634-3579
Cell: (603) 315-9010
Email: quintin.lee@eversource.com

Co-Vice Chairman: Michael Jones
Manager, Reliability Standards and Policy
National Grid
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

Sector 1 - Transmission Owners

Hydro One Networks, Inc.

Primary

Paul Malozewski, P. Eng., MBA, PMP
Senior Manager – Reliability Standards and
Compliance Assurance
Tel. 416-345-5005
Email: paul.malozewski@hydroone.com

Alternate

Payam Farahbakhsh, M. Eng, P. Eng.
Senior Network Management Engineer –
Reliability Standards and Compliance Assurance
Tel. (416) 345-5484
Email: Payam.Farahbakhsh@HydroOne.com

Consolidated Edison Company of New York, Inc.

Primary

Deidre Altobell
Chief Engineer, Transmission Planning
4 Irving Place
New York, NY 10003
Tel. (212) 460-3968
Fax (212) 529-1130
Email: altobelld@coned.com

Alternate

Martin Paszek
Manager, System Performance
Tel. (212) 460-6415
Fax (212) 529-1130
Email: paszekm@coned.com

National Grid

Primary

John Hastings
Lead Analyst, Transmission Control Center – NY
7437 Henry Clay Blvd HCB-3
Liverpool, NY 13088
National Grid, US
Tel. (315) 460-4139
Email: John.Hastings2@nationalgrid.com

Alternate

New Brunswick Power Corporation

Primary

Nurul Abser
Engineer IV, Compliance
Tel. (506) 458-3964
Cell. (506) 238-3624
Email: NAbser@nbpower.com

Alternate

Rob Vance
Senior Engineer, Corporate Compliance
Tel. (506) 458-3922
Email: rob.vance@NBPower.com

The United Illuminating Company

Primary

Michele Tondalo
Lead Analyst – NERC Compliance (O&P)
180 Marsh Hill Road
Orange, Connecticut 06477
Tel. (203) 499-2542
Email: Michele.Tondalo@uinet.com

Alternate

Michele Shafer
Lead Analyst – NERC Compliance
18 Link Dr.
Binghamton, New York 13904
Tel. (585) 484-6453
Cell. (607) 624-5984
Email: mshafer@nyseg.com

Hydro-Quebec TransÉnergie and Equipment

Primary

Nicolas Turcotte
Manager – RC Regulatory Affairs and
Compliance Implementation and Regulatory
Compliance
2 Complexe Desjardins, 13th floor, East Tower
Montréal, Québec, Canada H5B 1H7
Tel. (514) 798-1223
Ext :8795182
Email: turcotte.nicolas@hydro.qc.ca

Alternate

Stéphane Desbiens
Director – Reliability Standards & Regulatory
Compliance
2 Complexe Desjardins, 13th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 289-4435
Email: Desbiens.Stephane@hydro.qc.ca

Orange & Rockland Utilities, Inc.

Primary

Nick Kowalczyk
Chief System Operator
390 West Route 59
Spring Valley NY 10977
Tel. (845) 577-3796
Email: kowalczykn@oru.com

Alternate

Susmit Patel
Section Manager – Substation & Transmission
Engineering
Orange and Rockland Utilities Inc.
390 West Route 59
Spring Valley NY 10977
845-577-3203
Email: patels@oru.com

Eversource Energy

Primary

Quintin Lee
Program Manager - Reliability Compliance
Eversource Energy
780 North Commercial Street
Manchester, NH 03101
Office: (603) 634-3579
Cell: (603) 315-9010
Email: quintin.lee@eversource.com

Alternate

Sharon Flannery
Program Manager – Reliability Compliance
Eversource Energy
107 Selden Street
Berlin, CT
Office: (860) 665-5247
Cell: (860) 402-9157
Email: sharon.flannery@eversource.com

Central Hudson Gas & Electric

Primary

Michael Ridolfino
Engineer – Reliability Compliance
Office: (845) 486-5674
Cell: (845) 750-0896
Email: mridolfino@cenhud.com

Alternate

Sector (2) - Reliability Coordinators

New York Independent System Operator

Primary

James (Jim) Grant
Senior Reliability Engineer
Tel. (518) 356-6128
Email: jgrant@nyiso.com

Alternate

Gregory A. Campoli
Manager, Reliability Compliance & Industry
Affairs
Tel. (518) 356-6159
Email: gcampoli@nyiso.com

ISO New England, Inc.

Primary

John Pearson
Technical Manager
Tel. (413) 540-4260
Email: jpearson@iso-ne.com

Alternate

Kathleen M. Goodman
Senior Operations Compliance Coordinator
Tel. (413) 535-4111
Email: kgoodman@iso-ne.com

Independent Electricity System Operator

Primary

Helen Lainis
Senior Engineer/Technical Officer
Tel. (905) 855-4106
Email: helen.lainis@ieso.ca

Alternate

Sean Lagan
Compliance Analyst
Tel. (905) 855-6283
Email: sean.lagan@ieso.ca

Hydro-Quebec TransÉnergie and Equipment

Primary

Chantal Mazza
Reliability Standards Advisor III
2 Complexe Desjardins, 13th floor, East Tower
Montréal, Québec, Canada H5B 1H7
Tel. (514) 798-1223 Ext. 8795499
Email: mazza.chantal@hydro.qc.ca

Alternate

Junji Yamaguchi
Manager - Reliability Standards and Operating
Procedures
2 Complexe Desjardins, 13th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 289-2211 Ext. 2667
Email: Yamaguchi.junji@hydro.qc.ca

New Brunswick Power Corporation

Primary

Randy MacDonald
Director, Corporate Compliance
Tel. (506) 458-4653
Cell. (506) 470-3536
Email: RaMacDonald@NBPower.com

Alternate

Tim Hicks
Document & Compliance Coordinator
Tel. (506) 458-6511
Cell. (506) 238-3851
Email: Tim.Hicks@nbpower.com

Sector (3) - Transmission Dependent Utilities (“TDUs”); Distribution Companies and Load-Serving Entities (“LSEs”)

Consolidated Edison Company of New York, Inc.

Primary

Dermot Smyth
Senior Engineer
Tel. (212) 460-4093
Fax (212) 529-1130
Email: smythd@coned.com

Alternate

Lincoln Burton
Senior Engineer
Tel. (646) 660-3899
Fax (212) 529-1130
Email: burtonl@coned.com

National Grid

Primary

Michael Jones
Manager, Reliability Standards and Policy
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

Alternate

Orange & Rockland Utilities, Inc.

Primary

David Burke
Senior Specialist - Compliance
Tel. (845) 577-2841
Email: burkeda@oru.com

Alternate

Ben Wu
Principal Engineer
Transmission & Substation Engineering
Tel. (845) 577-3713
Email: wub@oru.com

Sector (4) - Generator Owners

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

Avani Pandya
Engineer
Fax (212) 529-1130
Email: pandyaa@coned.com

New York Power Authority

Primary

Salvatore Spagnolo
Program Manager, Reliability Standards & Compliance
Tel. (914) 390-8224
Mob. (347) 992-7015
Email: Salvatore.Spagnolo@nypa.gov

Alternate

Tom Savin
Program Manager, Reliability Standards & Compliance
Tel. (914) 287-3151
Email: Thomas.Savin@nypa.gov

Dominion Energy Services, Inc.

Primary

Sean Bodkin
NERC Compliance Policy Manager
Dominion Energy Services, Inc.
Tel. (804) 771-8429, tie line 8-786-8429
Cell: (804) 292-5721
Email: Sean.Bodkin@dominionenergy.com

Alternate

Connie Lowe
Regulatory and Market Policy Manager
Dominion Energy Services, Inc.
Tel. (804) 771-4447, tie 8-736-4447
Cell: 804-239-3201
Email: connie.lowe@dominionenergy.com

Ontario Power Generation, Inc.

Primary

Mike Cooke
Director – Reliability Compliance
Tel. (416) 592-6089
Cell: (905) 483-5520
Email: mike.cooke@opg.com

Alternate

David Kwan
Senior Regulatory Analyst
Tel. (416) 592-6369
Email: david.kwan@opg.com

Alternate

Constantin Chitescu
Regulatory Analyst
Tel. (416) 592-6055
Email: constantin.chitescu@opg.com

NextEra Energy, LLC

Primary

Silvia Parada Mitchell
Senior Director, Reliability Standards & Compliance
Tel. (561) 904-3767
Email: silvia.parada.mitchell@fpl.com

Alternate

Summer Esquerre
Director Reliability Standards & Compliance
Tel. (561) 904-3765
Email: summer.esquerre@fpl.com

Entergy Services, Inc

Primary

Glen Smith
NERC Compliance
Entergy Services, Inc
440 Hamilton Avenue
White Plains, NY 10601
914-272-3513
Email: gsmith@entergy.com

Alternate

Joel Plessinger
Manager, Operations & Planning Standards
NERC Compliance
Tel: (281)297-3644
Email: jplessi@entergy.com

PSEG

Primary

Sean Cavote
Director NERC Compliance
PSEG Law Department
80 Park Plaza, P3
Newark, NJ 07102-4194
973-430-5310
Email: sean.cavote@pseg.com

Alternate

Tim Kucey
Manager NERC Compliance
80 Park Plaza, P3
Newark, NJ 07102-4194
908-412-3078
Email: Timothy.Kucey@PSEG.com

Sector (5) - Marketers, Brokers and Aggregators

Consolidated Edison Company of New York, Inc.

Primary

Cristhian Godoy
Senior Engineer
4 Irving Place, New York, NY 10003
Tel. (917) 612-6364
Fax (212) 529-1130
Email: godoyc@coned.com

Alternate

Qinling Zheng
Engineer
Tel. (212) 460-2790
Fax (212) 529-1130
Email: zhengq@ConEd.com

Utility Services, Inc.

Primary

Brian Robinson
COO
Tel. (802) 241-1400
Email: brian.robinson@utilitysvcs.com

Alternate

Brian Evans-Mongeon
President/CEO
Tel. (802) 241-1400
Email: brian.evans-mongeon@utilitysvcs.com

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

New York Power Authority

Primary

Shivaz Chopra
Director, Reliability Standards & Compliance
Tel. (914) 681-6828
Tel. (914) 391-6839
Email: shivaz.chopra@nypa.gov

Alternate

Erick Barrios
Engineer, Reliability Standards & Compliance
Tel. (914) 681-6781
Tel. (914) 506-2152
Email: Erick.Barrios@nypa.gov

New York State Department of Public Service

Primary

Vijay Puran
Utility Supervisor, Bulk Electric Systems
Tel. (518) 486-5948
Email: vijay.puran@dps.ny.gov

Alternate

Jerry Ancona
Senior Engineer
Tel. (315) 448-7300
Email: Jerry.Ancona@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

Independent

Primary

David Kiguel
Independent Consultant
Toronto, Canada
Email: David.kiguel@outlook.com

Alternate

AESI, Inc.

Primary

Joel Charlebois
Vice President, Regulatory Compliance
Tel. (770) 870-1630 x 236
Cell: (718) 419-4012
Email: JoelC@aesi-inc.com

Alternate

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

North American Electric Reliability Corporation	))	Docket No. RC11-6-000

**NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION'S ANNUAL
REPORT ON THE FIND, FIX, TRACK AND REPORT AND COMPLIANCE
EXCEPTION PROGRAMS**

December 30, 2020

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	THE SUCCESSFUL EVOLUTION OF THE FFT AND CE PROGRAMS	3
III.	THE FFT AND CE PROGRAMS CONTINUE TO MEET EXPECTATIONS	6
IV.	FERC AND ERO ENTERPRISE STAFF COMMUNICATION AND COLLABORATION.....	8
V.	CONCLUSION	9

I. INTRODUCTION

The North American Electric Reliability Corporation (NERC), as the Electric Reliability Organization (ERO),¹ respectfully submits this filing as its annual report on the Find, Fix, Track and Report (FFT) and Compliance Exception (CE) programs. This filing complies with the Federal Energy Regulatory Commission's (FERC or the Commission) March 15, 2012 Order,² June 20, 2013 Order,³ and September 18, 2014 Order⁴ requiring an annual report on NERC's FFT program. This filing also combines the evaluation of CEs with the annual sampling of FFTs in compliance with the Commission's November 13, 2015 Order.⁵

Since 2011, the ERO Enterprise⁶ has used the FFT program to resolve about 2,772 instances of noncompliance with the NERC Reliability Standards, 81% of which posed a minimal risk to the reliability of the bulk power system (BPS).⁷ The Commission agreed that the FFT program has "produced efficiencies in NERC's processing of compliance and enforcement matters" and that continuing to use the FFT program to address moderate risk noncompliance will result in a "more efficient enforcement process and allow NERC and the Regional Entities to focus on occurrences of severe risk violations."⁸

¹ The Commission certified NERC as the ERO in accordance with section 215 of the Federal Power Act on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006), *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 *N. Am. Elec. Reliability Corp.*, 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 Order).

³ *N. Am. Elec. Reliability Corp.*, Order on Compliance Filing, 143 FERC ¶ 61,253 (2013) (June 2013 Order).

⁴ *N. Am. Elec. Reliability Corp.*, Order on Compliance Filing, 148 FERC ¶ 61,214 (2014) (September 2014 Order).

⁵ *N. Am. Elec. Reliability Corp.*, Docket No. RC11-6-004 (Nov. 13, 2015) (delegated letter order) (November 2015 Order).

⁶ The term "ERO Enterprise" refers to NERC and the six Regional Entities and NERC as a Compliance Enforcement Authority. The six Regional Entities are Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), ReliabilityFirst (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE), and Western Electricity Coordinating Council (WECC).

⁷ The numbers and percentages in this filing are from data as of October 30, 2020.

⁸ September 2014 Order at PP 1, 35.

Building on the success of the FFT program, the ERO Enterprise developed the CE program in February 2014 to streamline further the resolution of lesser-risk noncompliance with NERC Reliability Standards. The ERO Enterprise has resolved about 4,870 instances of noncompliance posing a minimal risk to the BPS through CEs since the inception of that program.⁹

In 2020, NERC and Commission staff completed their annual coordinated review of FFTs and CEs and found, as they had in previous reviews, that the ERO Enterprise appropriately handles noncompliance posing a minimal or moderate risk through these programs.¹⁰ NERC and Commission staff jointly sampled 62 FFTs and CEs, reviewed the associated supporting evidence, and agreed with all the final risk determinations. FERC staff noted that overall, the risk assessments have demonstrated a sustained improvement. Specifically, the assessments included clear explanations of potential risk, actual risk, and/or actual harm. FERC staff noted that the identification of root cause in FFTs and CEs has improved significantly over the past five years, moving from five percent missing an identification of root cause in 2015 to all noncompliance in this year's sampling including an identification of root cause.

⁹ See *supra* n.7.

¹⁰ See June 2013 Order, September 2014 Order, November 2015 Order, *N. Am. Elec. Reliability Corp.*, Docket No. RC11-6-005 (Jan. 13, 2017) (delegated letter order); *N. Am. Elec. Reliability Corp.*, Notice of Staff Review of Compliance Programs, Docket No. RC11-6-005 (Jun. 27, 2017); *N. Am. Elec. Reliability Corp.*, Order on Compliance Filing, 161 FERC ¶ 61,187 (2017), *N. Am. Elec. Reliability Corp.*, Docket No. RC11-6-006 (Dec. 6, 2017) (delegated letter order), *N. Am. Elec. Reliability Corp.*, Docket No. RC11-6-008 (Jan. 24, 2019) (delegated letter order).

II. THE SUCCESSFUL EVOLUTION OF THE FFT AND CE PROGRAMS

The FFT and CE programs are important elements of the ERO Enterprise's risk-based approach to enforcement.¹¹ The FFT program resolves noncompliance posing a minimal or moderate risk to the reliability of the BPS, while the CE program resolves noncompliance posing a minimal risk outside of Section 5.0 of the Compliance Monitoring and Enforcement Program (CMEP). Both programs require: (a) mitigation of the noncompliance; (b) availability of the facts and circumstances of the noncompliance for review by NERC and Applicable Governmental Authorities; (c) tracking and analysis of the noncompliance as necessary to identify broader risks; and (d) providing the opportunity for the registered entity to opt out of the disposition method.¹²

The FFT program was the first major step in implementing a risk-based approach to the enforcement of Reliability Standards that recognizes the fact that not all instances of noncompliance require the same type of processing and documentation. Over the last seven years, the FFT program evolved from a processing track limited to minimal risk noncompliance to a vehicle for increased efficient and effective disposition of moderate and minimal risk noncompliance. The success of the FFT program in resolving lesser risk noncompliance led to the expansion of the FFT program to include resolution of moderate risk noncompliance and the development of the CE program.

¹¹ For a description of NERC's enforcement processes, CEs, and FFTs, see NERC Rules of Procedure, App. 4C §§ 3.8, 3A.0, 3A.1, & 5.2A, respectively, available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20190125.pdf.

¹² See NERC Rules of Procedure, App. 4C §§ 5.2A and 3A, respectively.

Because of the FFT and CE programs, the ERO Enterprise is able to process minimal and moderate risk noncompliance more efficiently and effectively,¹³ thereby allowing the ERO Enterprise to focus its resources on noncompliance posing a greater risk to the reliability of the BPS. The ERO Enterprise’s use of the FFT and CE programs has continued to increase since FERC initially approved the programs. Since the inception of the FFT program, the number of moderate risk noncompliance processed as FFTs on average has been going up, as shown in Figure 1 below. The effective use of streamlined processing for lower risk noncompliance allows the ERO Enterprise to focus on higher risk issues.

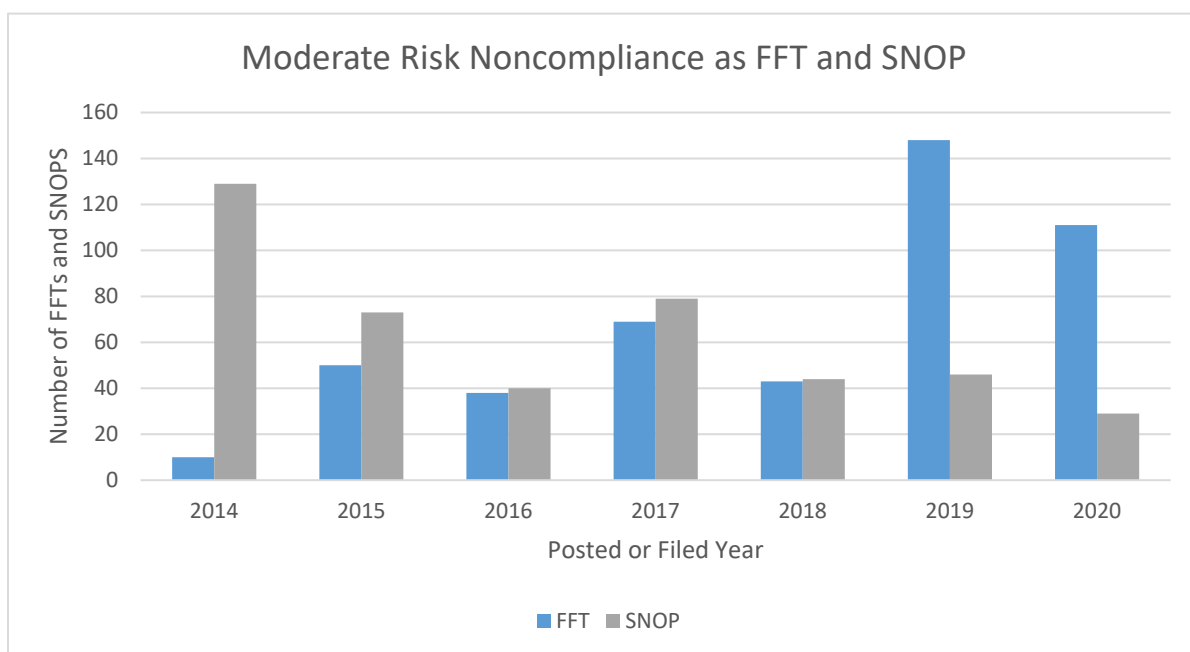


Figure 1: Moderate risk noncompliance processed as FFTs and SNOPs as of October 30, 2020

¹³ See September 2014 Order at PP 1, 25, n.37; see also *N. Am. Elec. Reliability Corp.*, NERC’s Annual Report on the Find, Fix, Track, and Report Program, Docket No. RC11-6-004, at 2 (Sept. 18, 2015); *N. Am. Elec. Reliability Corp.*, NERC’s Annual Report on the Find, Fix, Track, and Report and Compliance Exception Programs, Docket No. RC11-6-005, at 1-2 (Nov. 14, 2016); *N. Am. Elec. Reliability Corp.*, NERC’s Annual Report on the Find, Fix, Track and Report and Compliance Exception Programs, Docket No. RC11-6-000, at 1-2 (Oct. 4, 2017), and *N. Am. Elec. Reliability Corp.*, NERC’s Annual Report on the Find, Fix, Track and Report and Compliance Exception Programs, Docket No. RC11-6-008, at 1-2 (Nov. 1, 2018).

The number of minimal risk noncompliance processed as CEs has increased since 2016 and is the primary method of disposition for minimal risk noncompliance, as shown in Figure 2 below.

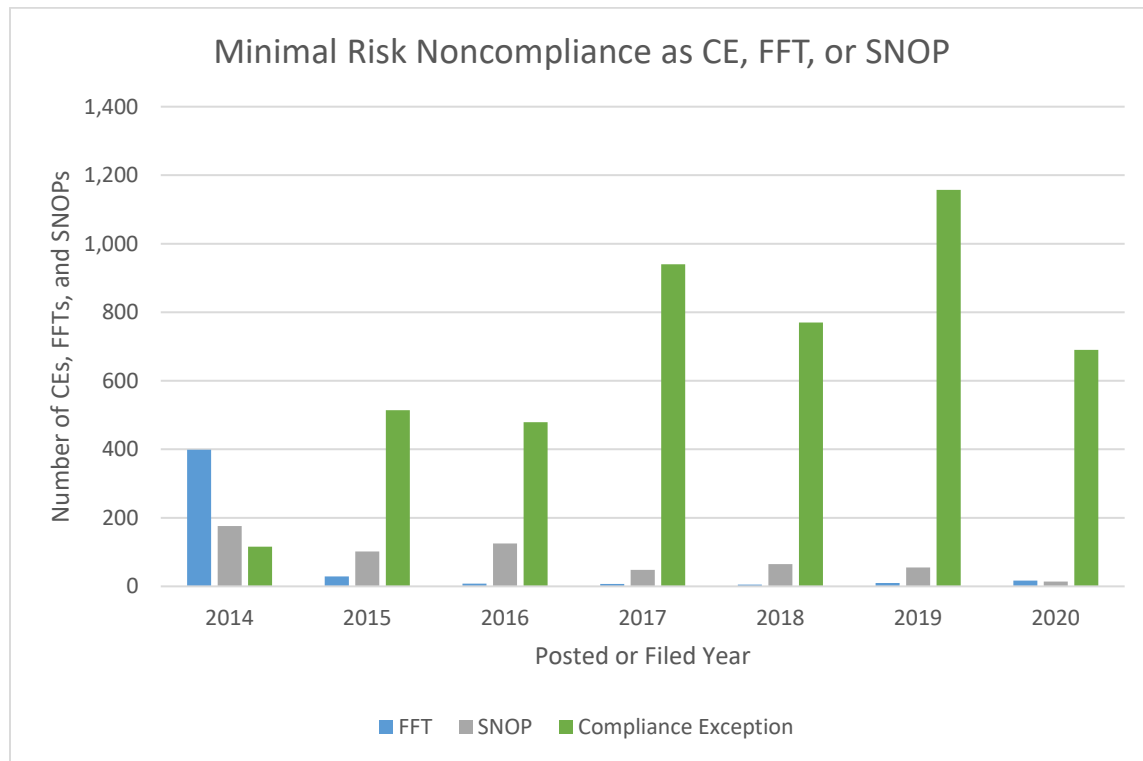


Figure 2: Minimal risk noncompliance processed as CEs, FFTs and SNOPs as of October 30, 2020.

As the ERO Enterprise has evolved in implementing risk-based CMEP, registered entities have also progressed, implementing more effective controls to improve compliance and maintain reliable and secure operations. The availability of dispositions not involving settlements or penalties makes registered entities more likely to conduct their own assessment of their compliance programs and possible noncompliance and, as a result, more likely to report noncompliance found during that assessment.

The Regional Entities' effective use of FFTs and CEs shows increased consistency in processing and understanding of the risk associated with individual noncompliance across the

ERO Enterprise. Further, risk-based enforcement, including the CE and FFT programs, encourages sustainable reliability and security through comprehensive mitigation that addresses root causes with the implementation of internal controls that reduce the likelihood of recurrence of the noncompliance.

III. THE FFT AND CE PROGRAMS CONTINUE TO MEET EXPECTATIONS

As part of their oversight of the FFT and CE programs, NERC and FERC staff conducted a joint review of FFTs and CEs posted by NERC between October 2018 and September 2019. The annual joint review began in October 2019 and ended in June 2020. During the review, NERC and FERC staff: (a) evaluated the Regional Entities' current FFT and CE procedures and processes;¹⁴ (b) reviewed a sample of minimal and moderate risk noncompliance processed as FFTs and CEs; (c) assessed successful completion of mitigation for FFTs and CEs requiring the performance of ongoing mitigation activities; (d) evaluated the Regional Entities' assessment of registered entities' internal controls; (e) identified region-specific best practices and areas for improvement; and (f) provided observations to the Regional Entities related to the completeness of the programs. Through this review, NERC and FERC staff determined whether the Regional Entities were successfully implementing the CMEP as it applies to the FFT and CE programs. NERC and FERC staff selected 24 FFTs and 38 CEs, weighted to the number of FFTs and CEs per Regional Entity.¹⁵ The selected sample included 18 CIP and 6 O&P FFTs and 19 CIP and 19 O&P CEs.¹⁶

¹⁴ FY2019 review included six Regional Entities and NERC in its role as a Compliance Enforcement Authority (collectively, the Regional Entities).

¹⁵ In FY2019 (October 1, 2018 to Sept. 30, 2019), NERC posted 102 FFTs (74 CIP and 28 O&P) and 957 CEs (503 CIP and 454 O&P) from six Regional Entities and NERC as a Compliance Enforcement Authority.

¹⁶ Using NERC's Sampling Guidelines, an independent population of 41-100 elements requires 23 samples. NERC and FERC agreed to include four additional FFTs. The guidelines are available at: http://www.nerc.com/pa/comp/Documents/Sampling_Handbook_Final_05292015.pdf. Similar to the method used for FFTs, according to NERC's Sampling Guidelines, an independent population of 101-1,000 elements requires 29 samples. NERC and FERC agreed to include an eight additional CEs.

On September 14, 2020, FERC staff issued its Notice of Staff Review of Enforcement Programs.¹⁷ FERC staff agreed with NERC that the FFT and CE programs are meeting expectations.¹⁸ FERC staff also agreed with the Regional Entities' final risk determinations for all samples.¹⁹ Overall, FERC staff noted that: (1) the risk assessments demonstrated a "significant improvement in the clear identification of factors affecting the risk prior to mitigation," specifically, all the assessments included clear explanations of potential risk, actual risk, and actual harm; and (2) the sampled noncompliance did not contain any material misrepresentations by the registered entities.²⁰

On June 17, 2020, NERC Enforcement staff provided individual feedback with specific findings and recommendations for each Regional Entity. NERC determined that all of the posted noncompliance were consistent with the evidence provided in response to the annual review. Additionally, all the affidavits required for noncompliance processed as FFTs were appropriately signed by officers within the companies. NERC determined that most descriptions of the noncompliance were adequate and included in the disposition documents, but there were some instances where additional details were included in supporting documents that could have provided more clarity in the CE and FFT descriptions. Overall, all the Regional Entities had detailed and thorough descriptions of the noncompliance and the Regional Entities provided detailed internal case notes to reflect their review and analysis of the noncompliance to determine risk and disposition.

¹⁷ *N. Am. Elec. Reliability Corp.*, Notice of Staff Review of Enforcement Programs, Docket No. RC11-6-010 (2020), available at https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20200914-3028.

¹⁸ *Id.* at p. 1.

¹⁹ *Id.* at p. 2.

²⁰ *Id.*

NERC Enforcement staff determined that the minor issues that were discovered did not affect the risk or disposition in any case. The dispositions generally included detailed risk statements with factors to support the assessed risk. In one case, NERC determined the posted risk assessment was generic and could have included additional mitigating factors to support the risk assessment. NERC provided feedback to Regional Entities that they should follow up with the registered entity if a notice of completion was not received in a timely manner. NERC also identified some areas of opportunities related to improvements in distinguishing where a prior noncompliance with the same or similar Standards could be indicative of a systemic issue. NERC shared Region-specific feedback with each Regional Entity, identifying positive feedback points and areas of improvement.

The results of the annual joint review show consistent improvement in program implementation. They also reflect significant alignment across the ERO Enterprise, particularly in the processing and understanding of the risk associated with individual noncompliance.

IV. FERC AND ERO ENTERPRISE STAFF COMMUNICATION AND COLLABORATION

In addition to the Annual FFT and CE Review, NERC and FERC staff conduct a 60-day review after posting of the FFTs and CEs.²¹ During this time, NERC and FERC staff reserve the right to withdraw or escalate any FFT or CE if it does not meet the requirements of the applicable programs. NERC and FERC staff communicate after the filing at the end of each month to address any concerns or questions that FERC staff might have. The review involves a

²¹ “In addition, the Commission retains the discretion to review a possible violation reported in an FFT informational filing even after the sixty day period if it finds that FFT treatment was obtained based on a material misrepresentation of the facts underlying the FFT matter.” March 2012 Order at P 72.

collaborative process where NERC and the Regional Entities provide responses to any concerns or questions within a few weeks after receiving the request.

V. CONCLUSION

NERC respectfully requests that the Commission accept this report in compliance with the March 2012 Order, June 2013 Order, September 2014 Order, and November 2015 Order.

Respectfully submitted,

/s/ James McGrane

Teresina Stasko
Assistant General Counsel and Director of
Enforcement
James McGrane
Senior Counsel
Harsimran Ahuja
Senior Enforcement Advisor
North American Electric Reliability
Corporation
1325 G. Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
teresina.stasko@nerc.net
james.mcgrane@nerc.net
simran.ahuja@nerc.net

Dated: December 30, 2020

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 December 2020.

/s/ James McGrane

James McGrane
*Senior Counsel for the North American
Electric Reliability Corporation*

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**North American Electric Reliability
Corporation**

)
)

Docket No. RD20-2-000

**INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY
CORPORATION REGARDING STANDARDS DEVELOPMENT PROJECTS**

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

December 15, 2020

TABLE OF CONTENTS

I. BACKGROUND.....	2
II. PROJECT SCHEDULES	2
III. CONCLUSION	2

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**North American Electric Reliability
Corporation**

)
)

Docket No. RD20-2-000

**INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY
CORPORATION REGARDING STANDARDS DEVELOPMENT PROJECTS**

Pursuant to paragraph 5 of the Order Directing Informational Filings Regarding NERC Standard Drafting Projects,¹ the North American Electric Reliability Corporation (“NERC”)² hereby submits to the Federal Energy Regulatory Commission (“FERC” or the “Commission”) an informational filing regarding two active Critical Infrastructure Protection (“CIP”) standard development projects: (1) Project 2016-02 – Modifications to CIP Standards (“Project 2016-02”); and (2) Project 2019-02 – BES Cyber System Information Access Management (“Project 2019-02”).³ Project 2016-02 focuses on modifications to the CIP Reliability Standards to incorporate applicable protections for virtualized environments. Project 2019-02 proposes to enhance the CIP standards by providing a secure path toward the use of third-party data storage and analysis systems and by clarifying the protections expected when using cloud computing services. This informational filing provides an update to the current schedules for both projects. NERC provided the initial informational filing regarding the schedules on March 19, 2020⁴ and two additional

¹ *N. Am. Elec. Reliability Corp.*, “Order Directing Informational Filings Regarding NERC Standard Drafting Projects,” 170 FERC ¶ 61,109 (Feb. 20, 2020) [hereinafter February 20 Order].

² The Commission certified NERC as the electric reliability organization (“ERO”) in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

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

⁴ NERC, *Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects*, Docket No. RD20-2-000 (March 19, 2020).

quarterly informational filings with updated schedules on June 19, 2020⁵ and September 17, 2020.⁶ NERC also provided a supplemental informational filing on November 13, 2020.⁷

I. BACKGROUND

In the February 20 Order, the Commission directed NERC to submit, within 30 days of the issuance of the Order, an informational filing that includes project schedules for Projects 2016-02 and 2019-02.⁸ The Commission stated that these schedules should include the status of the projects, interim target dates, and the anticipated filing date for new or modified Reliability Standards. In addition, the Commission directed NERC to file quarterly informational status updates, beginning in June 2020, until NERC files new or modified standards with the Commission.⁹

II. PROJECT SCHEDULES

The status of the projects, interim target dates, and the anticipated filing dates of the modified Reliability Standards for Projects 2016-02 and 2019-02 remain unchanged from those reported in the November Informational Filing. NERC notes that these schedules are projections and subject to change. Any changes will be reported in the next informational filing scheduled for March 2021.

III. CONCLUSION

At the time of this filing, Project 2016-02 and Project 2019-02 remain on schedule as provided herein. If any changes occur to the projects' status, target dates, or anticipated filing

⁵ NERC, *Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects*, Docket No. RD20-2-000 (June 19, 2020).

⁶ NERC, *Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects*, Docket No. RD20-2-000 (September 17, 2020) [hereinafter September Informational Filing].

⁷ NERC, *Supplemental Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects*, Docket No. RD20-2-000 (November 13, 2020) [hereinafter November Informational Filing].

⁸ February 20 Order, *supra* note 1, at P 5.

⁹ *Id.*

dates, NERC will provide these changes in its quarterly informational filings submitted pursuant to the directive in the February 20 Order.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

December 15, 2020

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 the above-referenced proceeding.

Dated at Washington, D.C. this 15th day of December, 2020.

/s/ Marisa Hecht

Marisa Hecht
*Counsel for North American
Electric Reliability Corporation*

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**WECC Regional Reliability Standard)
BAL-002-WECC-3 (Contingency Reserve))
)
)**

Docket No. RM19-20-000

**COMMENTS OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION AND
WESTERN ELECTRICITY COORDINATING COUNCIL
IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING**

The North American Electric Reliability Corporation (“NERC”) and Western Electricity Coordinating Council (“WECC”) hereby provide comments on the Notice of Proposed Rulemaking (“NOPR”) regarding proposed regional Reliability Standard BAL-002-WECC-3 issued by the Federal Energy Regulatory Commission (“FERC” or “Commission”) in this proceeding on October 15, 2020.¹ NERC is the Commission-certified electric reliability organization (“ERO”) responsible for the development and enforcement of mandatory Reliability Standards.² WECC is a Regional Entity that has been delegated authority under Section 215 of the Federal Power Act and Section 39.8 of the Commission’s regulations to propose regional Reliability Standards for the Western Interconnection.³

¹ Notice of Proposed Rulemaking, *WECC Regional Reliability Standard BAL-002-WECC-3 (Contingency Reserve)*, 173 FERC ¶ 61,032 (2020) [hereinafter the NOPR].

² The Commission certified NERC as the ERO in 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006), *order on reh’g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030 (2007), *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 Section 215 of the Federal Power Act, codified at 16 U.S.C. § 824o; 18 C.F.R. § 39.8. The Commission approved the currently effective delegation agreement in 2016 in Docket No. RR15-12-000. *See N. Am. Elec. Reliability Corp.*, 153 FERC ¶ 61,135 (2015) (conditionally approving revised delegation agreement and directing compliance filing), *order on compliance*, *N. Am. Elec. Reliability Corp.*, Docket No. RR15-12-001 (delegated letter

In the NOPR, the Commission proposes to approve proposed regional Reliability Standard BAL-002-WECC-3, in which NERC and WECC propose to retire Requirement R2 of the currently effective regional standard BAL-002-WECC-2a. While proposing to approve the standard, the Commission also states that it believes it is appropriate “to monitor the reliability impacts that the retirement of Requirement R2 may have on contingency reserves in the Western Interconnection.”⁴ The Commission therefore proposes to direct NERC and WECC to: (1) submit an informational filing 27 months following implementation of regional Reliability Standard BAL-002-WECC-3 that addresses the adequacy of contingency reserves in the Western Interconnection; and (2) make the Commission immediately aware of any adverse impacts resulting from the retirement of Requirement R2 that are discovered sooner, and any corrective actions taken or being considered.⁵

NERC and WECC support the Commission’s proposal to approve proposed Reliability Standard BAL-002-WECC-3. In these comments, NERC and WECC provide additional considerations for the Commission to consider in determining whether to direct further reporting following the implementation of the standard and the content of any required reports.

I. BACKGROUND

On September 6, 2019, NERC and WECC submitted a joint petition for approval of proposed regional Reliability Standard BAL-002-WECC-3 (Contingency Reserve).⁶ The proposed standard reflects the retirement of Requirement R2 in the currently effective regional standard BAL-002-WECC-2a. Regional Reliability Standard BAL-002-WECC-2a Requirement R2 requires each Reserve Sharing Group and each Balancing Authority that is not a member of a

order) (Mar. 23, 2016). A petition for approval of a revised delegation agreement to be effective January 1, 2021 is pending in Docket No. RR20-5-000.

⁴ NOPR at P 19.

⁵ *Id.*

⁶ *Joint Petition of NERC and WECC for Approval of Proposed Regional Reliability Standard BAL-002-WECC-3*, Docket No. RM19-20-000 (September 6, 2019) [hereinafter the Petition].

Reserve Sharing Group to maintain at least half of its minimum amount of Contingency Reserve as Operating Reserve-Spinning that meets certain defined characteristics. As explained further in NERC and WECC's Petition, WECC determined that Requirement R2 was no longer necessary following the implementation of continent-wide Reliability Standard BAL-003-1.1 Requirement R1 in 2016, and its continued retention alongside the continent-wide standard could lead to confusion and increased cost without additional reliability benefit.⁷ Based on the results of a field test, WECC determined that the retirement of regional Reliability Standard BAL-002-WECC-2a Requirement R2 is unlikely to have an adverse impact on reliability in the Western Interconnection.⁸

On October 15, 2020, the Commission issued the NOPR. In the NOPR, the Commission proposes to approve proposed regional Reliability Standard BAL-002-WECC-3.⁹ While proposing to approve the standard, the Commission stated that "unique aspects of contingency reserves in the Western Interconnection raise concerns about deliverability of contingency reserves within reserve sharing groups."¹⁰ In particular, the Commission noted that 32 out of 34 total Balancing Authorities in the WECC region are members of one of two reserve sharing groups. The Commission further stated that hydroelectric resources represent a significant share of the reserve sharing group contingency reserves for both groups, and that these resources "may or may not be deliverable to all member balancing authorities due to transmission constraints or limits on the hydro system."¹¹

⁷ Petition at 13.

⁸ Petition at 15. The field test results were discussed in detail in the Petition (see Petition at 14-15 and Exhibit C). On May 18, 2020, NERC and WECC submitted additional data to the Commission in response to a data request issued by the Director of the Office of Electric Reliability on February 18, 2020.

⁹ NOPR at P 17.

¹⁰ NOPR at P 18.

¹¹ *Id.*

Based on these considerations, the Commission believes that further monitoring is necessary. To that end, the Commission proposes to direct NERC and WECC to submit an informational filing 27 months following the implementation of proposed regional Reliability standard BAL-002-WECC-3. The Commission further proposes to direct NERC and WECC to “make the Commission immediately aware of any adverse impacts resulting from the retirement of Requirement R2, if they become apparent prior to the end of the reporting period, and any corrective actions taken or being considered.”¹²

The Commission states that NERC and WECC’s informational filing should include the following data:

1. for any reportable DCS event, the date, time and required amount of contingency reserves at the time of the event, the actual amount of Operating Reserves – Spinning at the time of the event, and the actual DCS performance;
2. for events involving a loss of 700 MW or greater, whether it is a reportable DCS event or not, the date and time of the event, the name of the resource(s), and the total MW;
3. the amount of spinning reserve above or below 50% during non-event times on an hourly basis for 24 months following implementation;
4. supporting data for NERC’s frequency response metric (Metric M-4) as it pertains to the Western Interconnection;
5. the DCS performance - as described in request (1) in the paragraph above - on a balancing authority basis; and
6. the hourly amount of contingency reserve and the fraction of that contingency reserve that is classified as spinning for each hour by balancing authority (not reserve sharing group).

NERC’s and WECC’s comments on the NOPR proposals are provided below.

II. COMMENTS

NERC and WECC support the Commission’s proposal to approve proposed Reliability Standard BAL-002-WECC-3. As the Commission states in the NOPR, NERC and WECC’s

¹² NOPR at P 19.

proposal is supported by the petition and the results of a field test, and the proposed standard, even without Requirement R2, will continue to provide more stringent requirements than those in the continent-wide disturbance control Reliability Standard BAL-002-3.¹³ While NERC and WECC do not believe that retiring Requirement R2 will result in any adverse reliability impacts based on the studies concluded to date, NERC and WECC are sensitive to the Commission's concerns regarding continued monitoring and do not oppose the Commission's proposal to direct further reporting following the implementation of proposed Reliability Standard BAL-002-WECC-3. NERC and WECC offer the following comments regarding the Commission's proposed reporting directive and respectfully request that these comments be considered by the Commission in issuing a final rule in this proceeding.

1. Requested Data

As discussed in the preceding section, the Commission proposes in the NOPR to direct NERC and WECC to submit six categories of data to be collected for 24 months following the implementation of Reliability Standard BAL-002-WECC-3. NERC and WECC offer the following comments on the proposed data collection.

NERC and WECC are concerned that, should the Commission adopt its proposed directive and direct NERC and WECC to report data on a Balancing Authority (and not just an aggregated Reserve Sharing Group) basis, the data that is ultimately reported to the Commission may not present a complete and accurate picture of conditions in the Western Interconnection. This is because U.S.-based Balancing Authorities may, through a Reserve Sharing Group, rely on spinning reserves carried by a Balancing Authority that is located outside the United States, beyond the reach of the Commission's jurisdiction. Data belonging or pertaining to such non-U.S. entities

¹³ See NOPR at P 17.

could not be provided to the Commission without the approval of that entity, which may or may not be granted. Consequently, NERC and WECC may only be able to provide U.S. Balancing Authority information and Reserve Sharing Group information that represents only the U.S. portion of the Reserve Sharing Group.

NERC and WECC also note that, to the extent Balancing Authorities and Reserve Sharing Groups determine the requested information is confidential, it may need to be filed on a non-public basis with the Commission.

2. Deadline for Reporting

In the NOPR, the Commission proposes to direct NERC and WECC to submit their informational filing 27 months following the implementation of proposed regional Reliability Standard BAL-002-WECC-3, and for this filing to contain 24 months of data. The Commission further states that the proposed informational filing report “can be drafted in a similar manner as the field test report provided in the petition including all of the requested data.”¹⁴

NERC and WECC appreciate the Commission’s guidance on the form of reporting to be provided to the Commission, should it adopt the proposed reporting directive. NERC and WECC are concerned that three months may not be sufficient to complete the validation and analysis of 24 months’ worth of the requested data in a report format. NERC and WECC submit that a deadline of 30 months following the implementation of proposed regional Reliability Standard BAL-002-WECC-3 would be more appropriate. In the interim, NERC and WECC would make the Commission “immediately aware of any adverse impacts resulting from the retirement of Requirement R2, if they become apparent” and report on “any corrective actions taken or being considered.”¹⁵

¹⁴ NOPR at 12 n.24.

¹⁵ NOPR at P 19.

III. CONCLUSION

NERC and WECC respectfully requests that the Commission accept these comments for consideration.

Respectfully submitted,

/s/ Lauren A. Perotti

Steve Goodwill
Vice President, General Counsel, and
Corporate Secretary
Chris Albrecht
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 582-0353
sgoodwill@wecc.org
calbrecht@wecc.org

*Counsel for the Western Electricity
Coordinating Council*

Lauren A. Perotti
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
lauren.perotti@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

Date: December 18, 2020

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 18^h day of December, 2020.

/s/ Lauren A. Perotti

Lauren A. Perotti

*Counsel for the North American Electric
Reliability Corporation*

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Californians for Green Nuclear Power, Inc.	)	Docket No. EL21-13-000
Complainant	)	
	)	
v.	)	
	)	
North American Electric Reliability	)	
Corporation,	)	
Western Electricity Coordinating Council,	)	
California Independent System Operator	)	
Corporation,	)	
California Public Utilities Commission,	)	
California State Water Resources Control	)	
Board,	)	
California State Lands Commission	)	
Respondents	)	

**THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION AND
THE WESTERN ELECTRICITY COORDINATING COUNCIL
JOINT ANSWER TO AMENDED COMPLAINT AND MOTION TO DISMISS**

Jordan White
Vice President of Strategic Engagement and
Deputy General Counsel
Chris Albrecht
Senior Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 582-0353
jwhite@wecc.org
calbrecht@wecc.org

Lauren Perotti
Senior Counsel
Marisa Hecht
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
marisa.hecht@nerc.net

*Counsel for the Western Electricity Coordinating
Council*

*Counsel for the North American Electric
Reliability Corporation*

December 15, 2020

TABLE OF CONTENTS

I.	NOTICES AND COMMUNICATIONS	3
II.	SUMMARY	3
A.	Background	3
B.	Summary of the Amended Complaint.....	4
C.	Summary of NERC and WECC Answer to Amended Complaint	5
III.	ANSWER TO AMENDED COMPLAINT AND MOTION TO DISMISS	6
A.	The Amended Complaint Should be Dismissed with Prejudice Because the Amended Complaint Exceeds the Statutory Authority Under Section 306 of the FPA.....	6
B.	The Amended Complaint Should be Dismissed with Prejudice Because it Fails to Meet the Minimum Requirements of the FPA and the Commission’s Regulations.	8
C.	NERC and WECC have Performed their Statutory Obligations Regarding Reliability Standards and Oversight.	12
IV.	CONCLUSION.....	15

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Californians for Green Nuclear Power, Inc.	)	Docket No. EL21-13-000
Complainant	)	
	)	
v.	)	
	)	
North American Electric Reliability	)	
Corporation,	)	
Western Electricity Coordinating Council,	)	
California Independent System Operator	)	
Corporation,	)	
California Public Utilities Commission,	)	
California State Water Resources Control	)	
Board,	)	
California State Lands Commission	)	
Respondents	)	

**THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION AND
THE WESTERN ELECTRICITY COORDINATING COUNCIL
JOINT ANSWER TO AMENDED COMPLAINT AND MOTION TO DISMISS**

Pursuant to Rules 206, 212, 213, and 215(b) of the Federal Energy Regulatory Commission’s (“FERC” or “Commission”) Rules of Practice and Procedure ¹ and the Commission’s Notice of Amended Complaint, ² the North American Electric Reliability Corporation (“NERC”) and the Western Electricity Coordinating Council (“WECC”) submit this Answer to the Amended Complaint filed by Californians for Green Nuclear Power, Inc.

¹ 18 C.F.R. §§ 385.206, 385.212, 385.213, and 385.215(b) (2020).

² Notice of Amended Complaint, Docket No. EL21-13-000 (November 30, 2020).

(“Complainant”) on November 25, 2020 in the above-captioned docket (“Amended Complaint”) and Motion to Dismiss.³

The Complaint alleges that (i) Respondents California Independent System Operator Corporation (“CAISO”), the California Public Utilities Commission (“CPUC”), the California State Water Resources Control Board (“CSWRCB”), and the California State Lands Commission (“CSLC”) have violated NERC’s Reliability Standards, specifically Reliability Standard BAL-002-WECC-2a (Contingency Reserve) through the approval of the retirement of the Diablo Canyon Power Plant (“DCPP”) planned in 2025; and (ii) Respondents NERC and WECC, as the Electric Reliability Organization (“ERO”) and a Regional Entity under the Federal Power Act (“FPA”),⁴ respectively, failed to conduct proper oversight or enforce NERC’s Reliability Standards, specifically BAL-002-WECC-2a, to prevent Reliability Standards violations caused by the retirement of the DCPP in 2025.⁵

As discussed below, the Commission should dismiss with prejudice the Amended Complaint against Respondents NERC and WECC for the following reasons: (i) the Amended Complaint exceeds the statutory authority of Section 306 of the FPA⁶ because NERC and WECC are not licensees, transmitting utilities, or public utilities; (ii) the Amended Complaint fails to meet the minimum requirements of the FPA and the Commission’s regulations by not specifying the basis in fact and law or the remedy requested; and (iii) the Amended Complaint fails on substantive

³ NERC and WECC have titled this document “Joint Answer to Amended Complaint and Motion to Dismiss.” However, NERC’s and WECC’s Answer is its Motion to Dismiss, because, as discussed below Complainant has no legal basis to file with FERC a complaint against NERC and WECC.

⁴ 16 U.S.C. §§ 791-828c.

⁵ Amended Complaint at 8.

⁶ 16 U.S.C. § 825e.

grounds because NERC and WECC have adhered to their duty to perform oversight and enforce Reliability Standards under the FPA.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:⁷

Jordan White*
Vice President of Strategic Engagement and
Deputy General Counsel
Chris Albrecht*
Senior Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 582-0353
jwhite@wecc.org
calbrecht@wecc.org

Lauren Perotti*
Senior Counsel
Marisa Hecht*
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
marisa.hecht@nerc.net

II. SUMMARY

A. Background

The Complainant submitted a complaint on October 26, 2020 (“Original Complaint”) in the above-captioned docket, listing NERC, WECC, CAISO, CPUC, CSWRCB, and CSLC as respondents. On November 16, 2020, NERC and WECC filed a joint answer to the Original Complaint (“Original Answer”) requesting the Commission dismiss the complaint. As described below, Complainant failed to satisfactorily address the points raised in the Original Answer. As such, NERC and WECC reiterate those arguments below, with the addition of a motion to dismiss and further demonstration that the Amended Complaint failed to cure the deficiencies detailed in the Original Answer.

⁷ Persons to be included on the Commission’s service list are identified by an asterisk. NERC and WECC respectfully request a waiver of Rule 203 of the Commission’s regulations, 18 C.F.R. § 385.203, to allow the inclusion of more than two persons on the service list in this proceeding.

B. Summary of the Amended Complaint

Complainant is a non-profit organization that takes issue with the CPUC's approval of a plan to retire DCPD in 2025.⁸ Regarding Respondents NERC and WECC, the Amended Complaint alleges that Respondents NERC and WECC "failed to conduct proper oversight or enforce NERC's [R]eliability [S]tandards to prevent [R]eliability [S]tandards violations caused by removing DCPD's 2240[sic] MW from the California electric grid."⁹ The Amended Complaint also alleges that Respondents have violated NERC's Reliability Standards, specifically BAL-002-WECC-2a, through the approval of the retirement of the DCPD planned in 2025.¹⁰ Finally, the Amended Complaint alleges the following: (i) CAISO's Loading Order, with CPUC affirmation, "...violate[s] FERC rules against unduly discriminatory and preferential treatment..."; and (ii) the "...totality of circumstances in California...make the federal rates...unjust and unreasonable under FPA sections 205 and 206."¹¹

The Amended Complaint requests that the Commission:

- i. Open investigations into the following:
 1. Determine the effect of retirement of DCPD on jurisdictional reliability (at 3)
 2. whether the closure of DCPD violates federal Reliability Standards; (at 3)
 3. how federal reliability standards for natural-gas pipelines could be affected by retirement of DCPD; (at 11)

⁸ Amended Complaint at 2.

⁹ *Id.* at 8.

¹⁰ *Id.* at 2, 5, and 8. The Amended Complaint does not specify which Respondents allegedly violated Reliability Standards.

¹¹ *Id.* at 3.

4. whether CAISO accepting closure of DCPD will result in market-design flaws; and (at 12)
5. whether CAISO is favoring renewable technologies (at 12)
- ii. Order a reliability analysis, including clarifying how DCPD mitigates against natural-gas system disruption; (at 11)
- iii. Take action to enforce NERC's Reliability Standards; and (at 8)
- iv. Consider whether whether jurisdictional rates are just and reasonable. (at 3)¹²

C. Summary of NERC and WECC Answer to Amended Complaint

The Commission should dismiss with prejudice the Amended Complaint against Respondents NERC and WECC and decline to provide the requested relief because: (i) NERC and WECC are not proper parties to a complaint under FPA Section 306, and the Amended Complaint exceeds the statutory authority pursuant to FPA Section 306; (ii) it fails to meet the minimum requirements applicable to complaints under the Commission's Rules of Practice and Procedure;¹³ and (iii) NERC and WECC satisfy their statutory and regulatory obligations under Section 215 of the FPA and the Commission's regulations. NERC and WECC raised these deficiencies in an answer to the Original Complaint, but the Complainant failed to cure those deficiencies in the Amended Complaint, as described in detail below. As such, NERC and WECC request the Commission grant the motion to dismiss the Amended Complaint.

¹²

Id. at 11.

¹³

See 18 C.F.R. § 385.206.

III. ANSWER TO AMENDED COMPLAINT AND MOTION TO DISMISS

A. **The Amended Complaint Should be Dismissed with Prejudice Because the Amended Complaint Exceeds the Statutory Authority Under Section 306 of the FPA.**

The Commission should dismiss the Amended Complaint because it exceeds the statutory authority of Section 306 of the FPA.¹⁴ Of the various statutes listed in the Amended Complaint, only the FPA is relevant to NERC and WECC.¹⁵ Complaints may be brought under FPA Section 306 regarding “anything done or omitted to be done by *any licensee, transmitting utility, or public utility* in contravention of the provisions” of the FPA.¹⁶ However, neither NERC, as the ERO under sections 215(a)(2) and (b) of the FPA,¹⁷ nor WECC, as a Regional Entity as defined in Section 215(a)(7) of the FPA,¹⁸ is considered a licensee, transmitting utility, or public utility. Neither NERC nor WECC (i) is licensed under Section 4 of the FPA;¹⁹ (ii) owns, operates, or controls facilities used for transmission;²⁰ or (iii) owns or operates facilities subject to the Commission’s jurisdiction.²¹ Accordingly, NERC and WECC are not proper parties to a complaint under FPA

¹⁴ 16 U.S.C. § 825e.

¹⁵ The Amended Complaint was noticed pursuant to the FPA, the Natural Gas Act of 1938, and the Federal Pipeline Safety Regulations, and Rule 206 of the Commission’s Rules of Practice and Procedure. *See* Notice of Amended Complaint, *supra*.

¹⁶ 16 U.S.C. § 825e (emphasis added).

¹⁷ *Id.* § 824o(a)(2) and (b). The Commission certified NERC as the ERO in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006), *order on reh’g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030 (2007), *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).

¹⁸ 16 U.S.C. § 824o(a)(7) and (e)(4). *See also N. Am. Elec. Reliability Corp.*, 119 FERC ¶ 61,060 (2006), *order on reh’g*, 120 FERC ¶ 61,260 (2007) (accepting a delegation agreement between NERC and WECC in order to designate WECC as a Regional Entity pursuant to Section 215(e)(4) of the FPA). The Commission approved the currently effective delegation agreement in 2016 in Docket No. RR15-12. *See N. Am. Elec. Reliability Corp.*, 153 FERC ¶ 61,135 (2015) (conditionally approving revised delegation agreement and directing compliance filing), *order on compliance*, *N. Am. Elec. Reliability Corp.*, Docket No. RR15-12-001 (delegated letter order) (Mar. 23, 2016). A petition for approval of a revised delegation agreement to be effective January 1, 2021 is pending in Docket No. RR20-5-000.

¹⁹ 16 U.S.C. § 796(5).

²⁰ *Id.* § 796(23).

²¹ *Id.* § 824(e).

Section 306, and the Amended Complaint against Respondents NERC and WECC must be dismissed as exceeding the authority provided under the statute.

Moreover, dismissing the Amended Complaint on these grounds is consistent with Commission precedent in similar cases. In *Morris v. N. Am. Elec. Reliability Corp. and SERC Reliability Corp.*, the Commission dismissed a complaint brought against NERC and another Regional Entity, finding that “[n]either [NERC nor the Regional Entity] serves as a licensee, transmitting utility, or public utility. Thus consistent with the plain words of the statute, and our precedent, we conclude that the complaint exceeds the statutory authority of section 306 of the FPA.”²²

Similarly, in *Citizens Energy Task Force v. Midwest Reliability Org., et al.*, the Commission dismissed a complaint against another Regional Entity, Midwest Reliability Organization (“MRO”), finding that MRO was “not a proper party to the Complaint.... MRO serves no other role under the FPA and is not a licensee, transmitting utility, or public utility. Thus,... the Complaint impermissibly exceeds the statutory authority of section 306 of the FPA.”²³

Furthermore, NERC and WECC raised this exact defense and Commission precedent in the Original Answer, and the Complainant failed to address this issue in the Amended Complaint. The Complainant does not present any precedent that counters *Morris v. N. Am. Elec. Reliability Corp. and SERC Reliability Corp.* or *Citizens Energy Task Force v. MRO*. While Complainant cites *Indicated Shippers v. Trunkline Gas Co. LLC* as permitting the Commission to exercise its discretion regardless of procedural deficiencies in a complaint, that discretion only applies to

²² *Morris v. N. Am. Elec. Reliability Corp. and SERC Reliability Corp.*, 153 FERC ¶ 61,266 at P 10 (2015) (dismissing a complaint alleging that NERC and SERC violated the NERC Rules of Procedure in assessing a penalty for Reliability Standards violations).

²³ *Citizens Energy Task Force v. MRO*, 144 FERC ¶ 61,006 at P 38.

waivers of requirements in the Commission's regulations.²⁴ In this case, it is the requirements in a statute, the FPA, that set forth an appropriate party to a complaint, and the Commission cannot waive statutory requirements. As such, consistent with the plain language of the statute and the Commission's precedent, the Commission should dismiss this Amended Complaint against NERC and WECC as it exceeds the statutory authority of Section 306 of the FPA.

B. The Amended Complaint Should be Dismissed with Prejudice Because it Fails to Meet the Minimum Requirements of the FPA and the Commission's Regulations.

The Commission should dismiss the Amended Complaint because it fails to meet the minimum requirements of the FPA and the Commission's regulations with respect to the content of complaints. To facilitate proceedings, the Commission sets forth procedural rules that dictate requirements for the content of complaints.²⁵ The purpose of these requirements is to help ensure respondents understand the specific allegations made in the complaint. Rule 203, for example, requires pleadings to set forth the basis in fact and law for the positions taken.²⁶ Rule 206 provides that complaints must, among other elements, (i) clearly identify the action or inaction alleged to violate applicable statutory or regulatory requirements; (ii) explain how the action or inaction violates applicable statutory standards or regulatory requirements; and (iii) state the specific relief or remedy requested and the basis for that relief.

Long-standing Commission precedent provides that "rather than bald allegations, [a complainant] must make an adequate proffer of evidence including pertinent information and

²⁴ Amended Complaint at 14 (citing *Indicated Shippers v. Trunkline Gas Co. LLC*, 105 FERC ¶ 61,394 (2003)).

²⁵ 18 C.F.R. § 385.

²⁶ *Id.* § 385.203(a)(7).

analysis to support its claims.”²⁷ Moreover, the precedent cited by Complainant, *Indicated Shippers v. Trunkline Gas Co. LLC*,²⁸ can be distinguished as the Commission waived the requirements to quantify the economic impact, whereas the deficiencies in the Amended Complaint go to the basis of the complaint itself. Further, the Commission has previously held that, in cases alleging a violation of a Reliability Standard, the complaint must set forth the specific Reliability Standard at issue and explain how the respondent’s action or inaction caused the violation. In *Citizens Energy Task Force v. Midwest Reliability Org., et al.*, the Commission held:

If a complaint regarding an alleged violation of a Reliability Standard is to meet the threshold requirements of Rule 206, then the complaint must, at a minimum, set forth the specific provision of the Reliability Standard that is at issue and provide some explanation as to how the Respondent’s alleged action or inaction caused the violation.²⁹

The Complaint failed to meet the necessary elements of Rule 206 and should therefore be dismissed for the following reasons.

First, the Complaint fails to “clearly identify the action or inaction” of NERC or WECC that allegedly violated applicable statutory or regulatory requirements or “explain how the action or inaction” violated applicable law. Instead, the Amended Complaint merely provides general, non-specific assertions that NERC and WECC “failed to conduct proper oversight or enforce NERC’s reliability standards to prevent reliability standards violations caused by removing

²⁷ *Ill. Muni. Elec. Agency v. Cent. Ill. Pub. Serv. Co.*, Order Dismissing Complaint Without Prejudice, 76 FERC ¶ 61,084 at 4 (1996); *CALifornians for Renewable Energy, Inc., (CARE) and Barbara Durkin v. Nat’l Grid, Cape Wind, and the Mass. Dep’t of Pub. Util.*, Order Dismissing Complaint, 137 FERC ¶ 61,113, at PP 2, 31-32 (2011); *CALifornians for Renewable Energy, Inc., Michael E. Boyd, and Robert M. Sarvey v. Pac. Gas and Elec. Co.*, Order Dismissing Complaint, 143 FERC ¶ 61,005 at P 2 (2013); and *Citizens Energy Task Force and Save Our Unique Lands v. Midwest Reliability Org., et al.*, Order Dismissing Complaint, 144 FERC ¶ 61,006 at P 38 (2013).

²⁸ Amended Complaint at 14 (citing *Indicated Shippers v. Trunkline Gas Co. LLC*, 105 FERC ¶ 61,394 (2003)).

²⁹ *Citizens Energy Task Force v. Midwest Reliability Org., et al.*, 144 FERC ¶ 61,006 at P 39 (2013).

DCPP's 2,240 MW from the California electric grid.”³⁰ These assertions are unsupported by any supporting evidence, information, or analysis.

In contrast to the Original Complaint, the Amended Complaint cites a specific standard, regional Reliability Standard BAL-002-WECC-2a, that was allegedly violated or that NERC and WECC allegedly failed to enforce. However, Commission precedent requires that a complaint “must, at a minimum, *set forth the specific provision* of the Reliability Standard.”³¹ The Complainant merely mentions BAL-002-WECC-2a and fails to state what requirement allegedly was violated or allegedly was not enforced. Moreover, the Complainant has failed to explain how the future planned retirement of DCPP has resulted in an applicable entity being unable to satisfy its obligations to maintain sufficient reserves in real-time operations.³²

Without the specificity required by Rule 206 and the Commission's precedent cited above, including in *Citizens Energy Task Force v. Midwest Reliability Org., et al.*, it is not possible for NERC and WECC to determine what action or inaction is the subject of the Amended Complaint. Notwithstanding the lack of specificity, NERC and WECC cannot even guess at the type of violation that is alleged when the Complainant alleges that a *future* action is causing violations of Real-time operations requirements.

NERC and WECC note that Section 215 of the FPA does not authorize the ERO or the Commission to set and enforce compliance with standards for adequacy of electric facilities or

³⁰ Amended Complaint at 8.

³¹ *Citizens Energy Task Force v. Midwest Reliability Org., et al.*, 144 FERC ¶ 61,006 at P 39 (2013) (emphasis added).

³² All of the requirements in BAL-002-WECC-2a are in the Real-time operations time horizon, which generally means the requirement concerns “actions required within one hour or less to preserve the reliability of the [BES].” NERC, “Time Horizons” (2014), https://www.nerc.com/pa/Stand/Resources/Documents/Time_Horizons.pdf. NERC and WECC note that Real-time is defined as “present time as opposed to future time” in the context of Reliability Standards. *Glossary of Terms Used in NERC Reliability Standards*, https://www.nerc.com/files/Glossary_of_Terms.pdf.

services.³³ Furthermore, the licensing and relicensing of nuclear generation plants is outside the authority of the ERO. As such, it is difficult to even infer the types of Reliability Standards violations the Complaint is trying to allege, including BAL-002-WECC-2a.

Second, the Amended Complaint did not state the “specific” relief or remedy requested and the basis for that relief as required by Rule 206. As noted previously, the Amended Complaint requests that the Commission take action to enforce NERC’s Reliability Standards, as well as review and initiate remediation of reliability concerns raised in the Complaint, among other requests that are not relevant to NERC and WECC.³⁴ However, by failing to identify the specific Reliability Standards provisions it seeks to be enforced, the Amended Complaint fails to state the specific relief or remedy requested and the basis for that relief, as required by Rule 206.

By requesting that FERC investigate “whether the closure of the DCPD violates federal Reliability Standards,”³⁵ the Amended Complaint: (i) demonstrates on its face that it fails to meet the requirement in Rule 206(b)(7) that it state a specific request for relief (as well as the requirements in Rule 206(b)(1) and (2) related to specific allegations), and (ii) undercuts the very basis upon which its allegations against NERC and WECC rely – that NERC and WECC failed to enforce Reliability Standards or exercise proper oversight.

³³ 16 U.S.C. § 824o(i)(2) (“This section does not authorize the ERO or the Commission to order the construction of additional generation or transmission capacity or to set and enforce compliance with standards for adequacy or safety of electric facilities or services.”). Additionally, 16 U.S.C. § 824o(a)(3) states, “The term ‘reliability standard’ means a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Finally, the Adequate Level of Reliability Task Force developed a technical report supporting the definition of Adequate Level of Reliability and providing guidance on the scope of Reliability Standards: https://www.nerc.com/comm/Other/Adequate%20Level%20of%20Reliability%20Task%20Force%20%20ALRTF%20DL/Final%20Documents%20Posted%20for%20Stakeholders%20and%20Board%20of%20Trustee%20Review/2013_03_26_Technical_Report_clean.pdf.

³⁴ Amended Complaint at 8.

³⁵ *Id.*

In conclusion, the Amended Complaint fails to meet the minimum requirements of Rule 206. The Amended Complaint did not clearly identify the NERC or WECC action or inaction that allegedly violated applicable law or explain how that action or inaction allegedly violated applicable law. The Amended Complaint also did not state the specific relief or remedy requested. Therefore, if the Commission does not dismiss the Amended Complaint because NERC and WECC are not proper parties to a complaint under Section 306 of the FPA, then the Commission should dismiss the Amended Complaint based on these procedural deficiencies.

C. NERC and WECC have Performed their Statutory Obligations Regarding Reliability Standards and Oversight.

NERC and WECC deny any and all allegations against them that could reasonably be inferred from the nonspecific assertions in the Amended Complaint and answer that they perform their duties as authorized and required by statute. By enacting the Energy Policy Act of 2005,³⁶ Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System, and with the duties of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. The Commission certified NERC as the ERO in 2006.³⁷ Similarly, the Commission accepted the delegation agreement designating WECC as a Regional Entity pursuant to FPA Section 215(e)(4).³⁸

³⁶ 16 U.S.C. § 824o.

³⁷ *N. Am. Elec. 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 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).

³⁸ 16 U.S.C. § 824o(a)(7) and (e)(4). *See also N. Am. Elec. Reliability Corp.*, 119 FERC ¶ 61,060 (2006), *order on reh'g*, 120 FERC ¶ 61,260 (2007) (accepting a delegation agreement between NERC and WECC in order to designate WECC as a Regional Entity pursuant to Section 215(e)(4) of the FPA).

As the ERO, NERC is committed to assure the reliability and security of the Bulk-Power System in North America.³⁹ Similarly, WECC supports this goal as a Regional Entity.⁴⁰ Under the FERC-approved NERC Rules of Procedure (“ROP”), NERC and WECC develop Reliability Standards in accordance with Section 300 (Reliability Standards Development) of the ROP, the NERC Standard Processes Manual, and the WECC Standard Development Procedures.⁴¹ NERC and the Regional Entities, including WECC, monitor, assess, and enforce compliance with Reliability Standards in the United States in accordance with Section 400 (Compliance Enforcement) of the ROP and the NERC Compliance Monitoring and Enforcement Program.⁴² Further, NERC and WECC perform assessments of the reliability and adequacy of the Bulk-Power System as required by Section 215(g) of the FPA⁴³ and Section 800 (Reliability Assessment and Performance Analysis) of the ROP.

Additionally, the Commission looks to ensure that NERC and WECC continue to meet their statutory and regulatory obligations. Recently, the Commission found that, “NERC continues to satisfy the statutory and regulatory criteria for certification as the ERO” and found that “the Regional Entities [including WECC] continue to satisfy applicable statutory and regulatory

³⁹ *N. Am. Elec. 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 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).

⁴⁰ *Id.*

⁴¹ The NERC Rules of Procedure are available at <https://www.nerc.com/AboutNERC/Pages/Rules-ofProcedure.aspx>. The NERC Standard Processes Manual is available at https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf. The WECC Reliability Standards Development Procedures are available at <https://www.wecc.org/Reliability/WECC%20Reliability%20Standards%20Development%20Procedures%20-%20FERC%20Approved%20October%2027%202017%20-%202019%20Template.pdf>.

⁴² *Id.* The NERC Compliance Monitoring and Enforcement Program is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_06082018.pdf.

⁴³ 16 U.S.C. § 824o(g).

criteria.”⁴⁴ While the Amended Complaint cited a NERC assessment⁴⁵ and a WECC assessment⁴⁶ that were not cited in the Original Complaint, NERC and WECC assert that these assessments demonstrate NERC and WECC carried out their duties pursuant to Section 800 of the ROP, even if the assessments do not come to the unit-specific conclusion the Complainant desires.

Therefore, to the extent that the Amended Complaint alleges that NERC and WECC have failed to satisfy their statutory and regulatory obligations in any way, NERC and WECC deny the allegations in their entirety and urge the Commission to dismiss the Amended Complaint.

⁴⁴ *N. Am. Elec. Reliability Corp.*, Order on Five-Year Performance Assessment, 170 FERC ¶ 61,029 at P 20 (2020).

⁴⁵ NERC, “2020-2021 Winter Reliability Assessment” (November 2020), https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_WRA_2020_2021.pdf.

⁴⁶ WECC, “Generation Resource Adequacy Forecast: Post-Transfers LOLH,” <https://www.wecc.org/ePubs/GenerationResourceAdequacyForecast/Pages/Post-Transfers-LOLH.aspx>.

IV. CONCLUSION

WHEREFORE, for the reasons stated above, NERC and WECC respectfully request that the Commission dismiss with prejudice the Amended Complaint against NERC and WECC, consistent with Section 306 of the FPA and Rule 206 of the Commission's rules.

Respectfully submitted,

/s/ Marisa Hecht

Jordan White
Vice President of Strategic Engagement and
Deputy General Counsel
Chris Albrecht
Senior Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 582-0353
jwhite@wecc.org
calbrecht@wecc.org

*Counsel for Western Electricity Coordinating
Council*

Lauren Perotti
Senior Counsel
Marisa Hecht
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
marisa.hecht@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

Date: December 15, 2020

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 15th day of December 2020.

/s/ Marisa Hecht
Marisa Hecht
*Counsel for the North American Electric
Reliability Corporation*

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**North American Electric Reliability
Corporation**

)

)

Docket No. RM20-17-000

**NOTICE OF WITHDRAWAL OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
FOR PROPOSED RELIABILITY STANDARD CIP-002-6**

Pursuant to Rule 216¹ of the Rules of Practice and Procedure of the Federal Energy Regulatory Commission (“FERC” or the “Commission”), the North American Electric Reliability Corporation (“NERC”) hereby submits this notice of withdrawal for proposed Reliability Standard CIP-002-6.

I. Background

On June 12, 2020, NERC submitted a petition for approval of proposed Reliability Standard CIP-002-6 in the above-captioned docket.² In the petition, NERC also sought the retirement of currently effective Reliability Standard CIP-002-5.1a. The Commission has not taken action on this filing as of the date of this notice.

II. Support for Withdrawal

At its February 4, 2021 meeting, the NERC Board of Trustees approved a resolution to withdraw proposed Reliability Standard CIP-002-6.³ NERC therefore asks the Commission to permit withdrawal of NERC’s June 12, 2020 petition seeking approval of proposed Reliability Standard CIP-002-6 and the retirement of currently effective Reliability Standard CIP-002-5.1a.

¹ 18 C.F.R. § 385.216 (2020).

² *Petition of NERC for Approval of Proposed Reliability Standard CIP-002-6*, Docket No. RM20-17-000 (June 12, 2020).

³ See NERC Board of Trustees February 4, 2021 Agenda Package Item 7.b, available at https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Open_Meeting_Agenda-Feb-4-2021_PUBLIC_ONLY.pdf.

In light of recent cybersecurity events and the evolving threat landscape, NERC asserts that additional caution is warranted regarding any criteria that may permit more entities to categorize Bulk Electric System (“BES”) Cyber Systems as low impact, such as the revisions proposed in CIP-002-6, and recommends further study. As a result, NERC withdraws proposed Reliability Standard CIP-002-6 until NERC has had the opportunity to reevaluate the criterion based on additional data and studies.

III. Conclusion

NERC requests that the Commission permit withdrawal of NERC’s June 12, 2020 petition seeking approval of proposed Reliability Standard CIP-002-6 and retirement of Reliability Standard CIP-002-5.1a, either by order or expiration of the 15-day period in Rule 216.

Respectfully submitted,

/s/ Marisa Hecht

Lauren A. Perotti
Senior Counsel
Marisa Hecht
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
marisa.hecht@nerc.net

*Counsel for the North American Electric Reliability
Corporation*

February 5, 2021

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 5th day of February, 2021.

/s/ Marisa Hecht

Marisa Hecht
*Counsel for the North American Electric Reliability
Corporation*

**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 ERRATA TO RELIABILITY STANDARD FAC-001-3**

Pursuant to Section 215(d)(1) of the Federal Power Act (“FPA”)¹ and Section 39.5² of the Federal Energy Regulatory Commission’s (“FERC” or “Commission”) regulations, the North American Electric Reliability Corporation (“NERC”)³ hereby submits for Commission approval errata to Reliability Standard FAC-001-3 (Facility Interconnection Requirements).

Exhibit A consists of a clean version of the proposed Reliability Standard and **Exhibit B** shows the proposed redlined changes. NERC requests that the Commission approve these errata changes as just, reasonable, not unduly discriminatory, and in the public interest.

I. Background

On April 20, 2016, NERC filed a petition seeking approval of Reliability Standards BAL-005-1 (Balancing Authority Control) and FAC-001-3 (Facility Interconnection Requirements), included as Exhibits A and B to the petition, respectively.⁴ NERC also sought approval of certain revised definitions of terms used in the NERC *Glossary of Terms used in Reliability Standards*, the associated implementation plans, violation risk factors and violation severity levels, and the retirement of certain Reliability Standards. On September 20, 2017, the Commission issued

¹ 16 U.S.C. § 824o.

² 18 C.F.R. § 39.5 (2020).

³ The Commission certified NERC as the electric reliability organization (“ERO”) in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

⁴ *Petition of NERC for Approval of Proposed Reliability Standards BAL-005-1 and FAC-001-3*, Docket No. RM16-13-000 (Apr. 20, 2016).

Order No. 836, in which it approved the Reliability Standards, definitions, and associated elements.⁵ Reliability Standard FAC-001-3 became effective in the United States on January 1, 2019.

It has come to NERC's attention that NERC inadvertently filed a draft version of the FAC-001-3 Reliability Standard as Exhibit B to its April 20, 2016 petition, instead of the final version that was approved by the NERC ballot body and adopted by the NERC Board of Trustees in February 2016.⁶ The version filed as Exhibit B to NERC's April 20, 2016 petition did not reflect certain non-substantive revisions in Requirement R3 Part 3.3 and Requirement R4 Part 4.3 that were made prior to the final ballot for the standard. The final language for these Requirement Parts was accurately reflected in the retirement-by-retirement justification for the standard contained in the main body of NERC's petition.⁷

To promote consistency and clarity as to the mandatory and effective language, NERC respectfully requests that the Commission approve the NERC Board-adopted version of the FAC-001-3 Reliability Standard attached as **Exhibit A** to this filing. The differences between the two versions of the standard are noted in the following section.

II. Errata

Prior to the final ballot for Reliability Standard FAC-001-3, the standard drafting team made certain clarifying revisions in Requirement R3 Part 3.3 and Requirement R4 Part 4.3,

⁵ *Balancing Authority Control, Inadvertent Interchange, and Facility Interconnection Reliability Standards*, 160 FERC ¶ 61,070 (2017).

⁶ See NERC Board of Trustees, February 11, 2016 Agenda Package, item 4a, available at <https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/BOT%20-%20February%2011%202016%20Agenda%20Package.pdf>. See also Minutes of the NERC Board of Trustees February 11, 2016 Meeting, available at <https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/BOT%20-%20February%2011%202016%20Minutes.pdf>.

⁷ See April 20, 2016 Petition at 22-23. The final version was also included in Exhibit N, Summary of Development History and Complete Record of Development (item 74).

which were new subparts in Reliability Standard FAC-001-3. This language was part of the version that was ultimately approved by the ballot pool and adopted by the NERC Board of Trustees, and which is attached as **Exhibit A** to this petition.

As noted above, the language of the final version was accurately reflected in the main body of NERC's April 20, 2016 petition. The differences between the draft version attached as Exhibit B to NERC's April 20, 2016 petition and the final version attached to this petition are shown below:

- R3.** Each Transmission Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower]*
[Time Horizon: Long-Term Planning]

3.3. Procedures for confirming with those responsible for the reliability of affected systems ~~of that~~ new or materially modified ~~transmission~~ Facilities are within a Balancing Authority Area's metered boundaries.

- R4.** Each applicable Generator Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower]* *[Time Horizon: Long-Term Planning]*

4.3. Procedures for confirming with those responsible for the reliability of affected systems ~~of that~~ new or materially modified ~~generation~~ Facilities are within a Balancing Authority Area's metered boundaries.

As explained in the record of development filed with NERC's April 20, 2016 petition, the standard drafting team determined to remove before the final ballot the word "transmission" from draft Requirement R3.3, and the word "generation" from draft Requirement R4.4, to more clearly reflect the intent of the drafting team that a Transmission Owner or Generator Owner

properly address procedures for confirming that those responsible for reliability of the applicable affected systems are within a Balancing Authority Area's metered boundaries.⁸

Approval of the attached version of the FAC-008-3 standard will promote consistency and clarity as to the mandatory and effective language, and is just, reasonable, not unduly discriminatory, and in the public interest.

III. Notices and Communications

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

Lauren A. Perotti
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
lauren.perotti@nerc.net

Howard Gugel
Vice President, Engineering and 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
howard.gugel@nerc.net

⁸ April 20, 2016 Petition, Exhibit N at item 24 (pdf at 1342) (January 28, 2016 Consideration of Comments at 65).

IV. Conclusion

For the reasons set forth above, NERC respectfully requests that the Commission approve the proposed errata to Reliability Standard FAC-001-3, included in **Exhibit A**.

Respectfully submitted,

/s/ Lauren A. Perotti

Lauren A. Perotti
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
lauren.perotti@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

January 7, 2021

EXHIBITS

Exhibit A Proposed Reliability Standard FAC-001-3 - clean

As adopted by the NERC Board of Trustees

Exhibit B Proposed Reliability Standard FAC-001-3 – redline

showing changes to the version filed with the April 20, 2016 Petition

Exhibit A

Proposed Reliability Standard FAC-001-3 – clean
As adopted by the NERC Board of Trustees

A. Introduction

1. **Title:** Facility Interconnection Requirements
2. **Number:** FAC-001-3
3. **Purpose:** To avoid adverse impacts on the reliability of the Bulk Electric System, Transmission Owners and applicable Generator Owners must document and make Facility interconnection requirements available so that entities seeking to interconnect will have the necessary information.
4. **Applicability:**
 - 4.1. **Functional Entities:**
 - 4.1.1 Transmission Owner
 - 4.1.2 Applicable Generator Owner
 - 4.1.2.1 Generator 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.
5. **Effective Date:** See Implementation Plan for FAC-001-3.

B. Requirements and Measures

- R1.** Each Transmission Owner shall document Facility interconnection requirements, update them as needed, and make them available upon request. Each Transmission Owner's Facility interconnection requirements shall address interconnection requirements for: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*
 - 1.1. generation Facilities;
 - 1.2. transmission Facilities; and
 - 1.3. end-user Facilities.
- M1.** Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R1.
- R2.** Each applicable Generator Owner shall document Facility interconnection requirements and make them available upon request within 45 calendar days of full execution of an 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. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*
- M2.** Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R2.

- R3.** Each Transmission Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*
- 3.1.** Procedures for coordinated studies of new or materially modified existing interconnections and their impacts on affected system(s).
 - 3.2.** Procedures for notifying those responsible for the reliability of affected system(s) of new or materially modified existing interconnections.
 - 3.3.** Procedures for confirming with those responsible for the reliability of affected systems that new or materially modified Facilities are within a Balancing Authority Area’s metered boundaries.
- M3.** Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R3.
- R4.** Each applicable Generator Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*
- 4.1.** Procedures for coordinated studies of new interconnections and their impacts on affected system(s).
 - 4.2.** Procedures for notifying those responsible for the reliability of affected system(s) of new interconnections.
 - 4.3.** Procedures for confirming with those responsible for the reliability of affected systems that new or materially modified Facilities are within a Balancing Authority Area’s metered boundaries.
- M4.** Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R4.

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 applicable Functional 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:

The responsible entities shall retain documentation as evidence for three 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 Audit

Self-Certification

Spot Check

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Lower	N/A	The Transmission Owner documented Facility interconnection requirements and updated them as needed, but failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements and made them available upon request, but failed to update them as needed. OR The Transmission Owner documented Facility interconnection requirements, updated them as needed, and made them available upon request, but	The Transmission Owner documented Facility interconnection requirements, but failed to update them as needed and failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements, updated them as needed, and made them available upon request, but failed to address interconnection requirements for two of the Facilities as specified in R1, Parts 1.1, 1.2, or 1.3.	The Transmission Owner did not document Facility interconnection requirements.

				failed to address interconnection requirements for one of the Facilities as specified in R1, Parts 1.1, 1.2, or 1.3.		
R2	Long-term Planning	Lower	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 45 calendar days but less than or equal to 60 calendar days after full execution of an 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.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 60 calendar days but less than or equal to 70 calendar days after full execution of an 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.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 70 calendar days but less than or equal to 80 calendar days after full execution of an 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.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 80 calendar days after full execution of an 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.

R3	Long-term Planning	Lower	N/A	The Transmission Owner failed to address one part of Requirement R3 Part 3.1 through Part 3.3.	The Transmission Owner failed to address two parts of Requirement R3 Part 3.1 through Part 3.3.	The Transmission Owner failed to address Requirement R3 Part 3.1 through Part 3.3.
R4	Long-term Planning	Lower	N/A	The Generator Owner failed to address one part of Requirement R4 Part 4.1 through Part 4.3.	The Generator Owner failed to address two parts of Requirement R4 Part 4.1 through Part 4.3.	The Generator Owner failed to address Requirement R4 Part 4.1 through Part 4.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1		Added requirements for Generator Owner and brought overall standard format up to date.	Revision under Project 2010-07
1	February 9, 2012	Adopted by the Board of Trustees	
1	September 19, 2013	A FERC order was issued on September 19, 2013, approving FAC-001-1. This standard became enforceable on November 25, 2013 for Transmission Owners. For Generator Owners, the standard becomes enforceable on January 1, 2015.	
2		Revisions to implement the recommendations of the FAC Five-Year Review Team.	Revision under Project 2010-02
2	August 14, 2014	Adopted by the Board of Trustees	
2	November 6, 2014	FERC letter order issued approving FAC-001-2.	
3	February 11, 2016	Adopted by the Board of Trustees	Moved BAL-005-0.2b Requirement R1 into FAC-001-3 Requirements R3 and R4
3	September 20, 2017	FERC Order No. 836 issued approving FAC-001-3	
3	TBD	Errata	

Guidelines and Technical Basis

Entities should have documentation to support the technical rationale for determining whether an existing interconnection was “materially modified.” Recognizing that what constitutes a “material modification” will vary from entity to entity, the intent is for this determination to be based on engineering judgment.

Requirement R3:

Originally the Parts of R3, with the exception of the first two bullets, which were added by the Project 2010-02 drafting team, this list has been moved to the Guidelines and Technical Basis section to provide entities with the flexibility to determine the Facility interconnection requirements that are technically appropriate for their respective Facilities. Including them as Parts of R3 was deemed too prescriptive, as frequently some items in the list do not apply to all applicable entities – and some applicable entities will have requirements that are not included in this list.

Each Transmission Owner and applicable Generator Owner should consider the following items in the development of Facility interconnection requirements:

- Procedures for requesting a new Facility interconnection or material modification to an existing interconnection
- Data required to properly study the interconnection
- Voltage level and MW and MVAR capacity or demand at the point of interconnection
- Breaker duty and surge protection
- System protection and coordination
- Metering and telecommunications
- Grounding and safety issues
- Insulation and insulation coordination
- Voltage, Reactive Power (including specifications for minimum static and dynamic reactive power requirements), and power factor control
- Power quality impacts
- Equipment ratings
- Synchronizing of Facilities
- Maintenance coordination
- Operational issues (abnormal frequency and voltages)
- Inspection requirements for new or materially modified existing interconnections
- Communications and procedures during normal and emergency operating conditions

Rationale

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

Rationale for Requirement R3.3: Consistent with the Functional Model, there cannot be an assumption that the entity owning the transmission will be the same entity providing the BA function. It is the responsibility of the party interconnecting to make appropriate arrangements with a Balancing Authority to ensure its Facilities are within the BA's metered boundaries, which also serves to facilitate the process of the coordination between the two entities that will be required under numerous other standards upon the start of operation. Under 3.3, the Transmission Owner is responsible for confirming that the party interconnecting has made appropriate provisions with a Balancing Authority to operate within its metered boundaries.

Rationale for Requirement R4.3: Consistent with the Functional Model, there cannot be an assumption that the entity owning the generation will be the same entity providing the BA function. It is the responsibility of the party interconnecting to make appropriate arrangements with a Balancing Authority to ensure its Facilities are within the BA's metered boundaries, which also serves to facilitate the process of the coordination between the two entities that will be required under numerous other standards upon the start of operation. Under 4.3, the Generator Owner is responsible for confirming that the party interconnecting has made appropriate provisions with a Balancing Authority to operate within its metered boundaries.

Exhibit B

Proposed Reliability Standard FAC-001-3 – redline
Showing changes to the version filed with the April 20, 2016 Petition

A. Introduction

1. **Title:** **Facility Interconnection Requirements**
2. **Number:** FAC-001-3
3. **Purpose:** To avoid adverse impacts on the reliability of the Bulk Electric System, Transmission Owners and applicable Generator Owners must document and make Facility interconnection requirements available so that entities seeking to interconnect will have the necessary information.
4. **Applicability:**
 - 4.1. **Functional Entities:**
 - 4.1.1 Transmission Owner
 - 4.1.2 Applicable Generator Owner
 - 4.1.2.1 Generator 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.
5. **Effective Date:** See Implementation Plan for FAC-001-3.

B. Requirements and Measures

- R1.** Each Transmission Owner shall document Facility interconnection requirements, update them as needed, and make them available upon request. Each Transmission Owner's Facility interconnection requirements shall address interconnection requirements for: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*
 - 1.1. generation Facilities;
 - 1.2. transmission Facilities; and
 - 1.3. end-user Facilities.
- M1.** Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R1.
- R2.** Each applicable Generator Owner shall document Facility interconnection requirements and make them available upon request within 45 calendar days of full execution of an 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. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*
- M2.** Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R2.

- R3.** Each Transmission Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*
- 3.1.** Procedures for coordinated studies of new or materially modified existing interconnections and their impacts on affected system(s).
 - 3.2.** Procedures for notifying those responsible for the reliability of affected system(s) of new or materially modified existing interconnections.
 - 3.3.** Procedures for confirming with those responsible for the reliability of affected systems ~~of that~~ new or materially modified ~~transmission~~ Facilities are within a Balancing Authority Area’s metered boundaries.
- M3.** Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R3.
- R4.** Each applicable Generator Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*
- 4.1.** Procedures for coordinated studies of new interconnections and their impacts on affected system(s).
 - 4.2.** Procedures for notifying those responsible for the reliability of affected system(s) of new interconnections.
 - 4.3.** Procedures for confirming with those responsible for the reliability of affected systems ~~of that~~ new or materially modified ~~generation~~ Facilities are within a Balancing Authority Area’s metered boundaries.
- M4.** Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R4.

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 applicable Functional 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:

The responsible entities shall retain documentation as evidence for three 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 Audit

Self-Certification

Spot Check

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Lower	N/A	The Transmission Owner documented Facility interconnection requirements and updated them as needed, but failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements and made them available upon request, but failed to update them as needed. OR The Transmission Owner documented Facility interconnection requirements, updated them as needed, and made them available upon request, but	The Transmission Owner documented Facility interconnection requirements, but failed to update them as needed and failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements, updated them as needed, and made them available upon request, but failed to address interconnection requirements for two of the Facilities as specified in R1, Parts 1.1, 1.2, or 1.3.	The Transmission Owner did not document Facility interconnection requirements.

				failed to address interconnection requirements for one of the Facilities as specified in R1, Parts 1.1, 1.2, or 1.3.		
R2	Long-term Planning	Lower	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 45 calendar days but less than or equal to 60 calendar days after full execution of an 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.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 60 calendar days but less than or equal to 70 calendar days after full execution of an 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.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 70 calendar days but less than or equal to 80 calendar days after full execution of an 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.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 80 calendar days after full execution of an 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.

R3	Long-term Planning	Lower	N/A	The Transmission Owner failed to address one part of Requirement R3 Part 3.1 through Part 3.3.	The Transmission Owner failed to address two parts of Requirement R3 Part 3.1 through Part 3.3.	The Transmission Owner failed to address Requirement R3 Part 3.1 through Part 3.3.
R4	Long-term Planning	Lower	N/A	The Generator Owner failed to address one part of Requirement R4 Part 4.1 through Part 4.3.	The Generator Owner failed to address two parts of Requirement R4 Part 4.1 through Part 4.3.	The Generator Owner failed to address Requirement R4 Part 4.1 through Part 4.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1		Added requirements for Generator Owner and brought overall standard format up to date.	Revision under Project 2010-07
1	February 9, 2012	Adopted by the Board of Trustees	
1	September 19, 2013	A FERC order was issued on September 19, 2013, approving FAC-001-1. This standard became enforceable on November 25, 2013 for Transmission Owners. For Generator Owners, the standard becomes enforceable on January 1, 2015.	
2		Revisions to implement the recommendations of the FAC Five-Year Review Team.	Revision under Project 2010-02
2	August 14, 2014	Adopted by the Board of Trustees	
2	November 6, 2014	FERC letter order issued approving FAC-001-2.	
3	February 11, 2016	Adopted by the Board of Trustees	Moved BAL-005-0.2b Requirement R1 into FAC-001-3 Requirements R3 and R4
3	September 20, 2017	FERC Order No. 836 issued approving FAC-001-3	
<u>3</u>	<u>TBD</u>	<u>Errata</u>	

Guidelines and Technical Basis

Entities should have documentation to support the technical rationale for determining whether an existing interconnection was “materially modified.” Recognizing that what constitutes a “material modification” will vary from entity to entity, the intent is for this determination to be based on engineering judgment.

Requirement R3:

Originally the Parts of R3, with the exception of the first two bullets, which were added by the Project 2010-02 drafting team, this list has been moved to the Guidelines and Technical Basis section to provide entities with the flexibility to determine the Facility interconnection requirements that are technically appropriate for their respective Facilities. Including them as Parts of R3 was deemed too prescriptive, as frequently some items in the list do not apply to all applicable entities – and some applicable entities will have requirements that are not included in this list.

Each Transmission Owner and applicable Generator Owner should consider the following items in the development of Facility interconnection requirements:

- Procedures for requesting a new Facility interconnection or material modification to an existing interconnection
- Data required to properly study the interconnection
- Voltage level and MW and MVAR capacity or demand at the point of interconnection
- Breaker duty and surge protection
- System protection and coordination
- Metering and telecommunications
- Grounding and safety issues
- Insulation and insulation coordination
- Voltage, Reactive Power (including specifications for minimum static and dynamic reactive power requirements), and power factor control
- Power quality impacts
- Equipment ratings
- Synchronizing of Facilities
- Maintenance coordination
- Operational issues (abnormal frequency and voltages)
- Inspection requirements for new or materially modified existing interconnections
- Communications and procedures during normal and emergency operating conditions

Rationale

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

Rationale for Requirement R3.3: Consistent with the Functional Model, there cannot be an assumption that the entity owning the transmission will be the same entity providing the BA function. It is the responsibility of the party interconnecting to make appropriate arrangements with a Balancing Authority to ensure its Facilities are within the BA's metered boundaries, which also serves to facilitate the process of the coordination between the two entities that will be required under numerous other standards upon the start of operation. Under 3.3, the Transmission Owner is responsible for confirming that the party interconnecting has made appropriate provisions with a Balancing Authority to operate within its metered boundaries.

Rationale for Requirement R4.3: Consistent with the Functional Model, there cannot be an assumption that the entity owning the generation will be the same entity providing the BA function. It is the responsibility of the party interconnecting to make appropriate arrangements with a Balancing Authority to ensure its Facilities are within the BA's metered boundaries, which also serves to facilitate the process of the coordination between the two entities that will be required under numerous other standards upon the start of operation. Under 4.3, the Generator Owner is responsible for confirming that the party interconnecting has made appropriate provisions with a Balancing Authority to operate within its metered boundaries.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

OFFICE OF ELECTRIC RELIABILITY

North American Electric Reliability Corporation
Docket No. RD21-1-000

December 23, 2020

North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, D.C. 20005

Attention: Lauren A. Perotti, Senior Counsel
North American Electric Reliability Corporation
Steve Goodwill, Senior Vice President of Reliability and Security
Oversight, General Counsel, and Corporate Secretary
Western Electricity Coordinating Council

Reference: Joint Petition of the North American Electric Reliability Corporation and
Western Electricity Coordinating Council for Approval of Proposed
Reliability Standard PRC-006-5

Dear Ms. Perotti and Mr. Goodwill:

On October 27, 2020, the North American Electric Reliability Corporation (NERC) and Western Electricity Coordinating Council (WECC) filed a joint petition seeking approval of proposed Reliability Standard PRC-006-5 (Automatic Underfrequency Load Shedding).

Proposed Reliability Standard PRC-006-5 includes revisions to the WECC regional Variance that clarify applicability of continent-wide requirements to entities in the Western Interconnection and clarify the applicability of the WECC regional Variance to Planning Coordinators. The continent-wide requirements were not changed substantively from Reliability Standard PRC-006-4. The WECC regional Variance complements the continent-wide system performance levels by requiring further coordination among entities providing Planning Coordinator services in the Western Interconnection.

WECC developed the proposed revisions to the regional Variance in proposed Reliability Standard PRC-006-5 to further promote the coordinated planning and

operation of the interconnected Bulk-Power System. The proposed revisions to the WECC regional Variance include: (1) clarifying that Requirements R14 and R15 of the continent-wide Reliability Standard do not apply to entities in the Western Interconnection; (2) clarifying that the use of “Planning Coordinator” in the WECC regional Variance is specific to those providing Planning Coordinator services to Registered Entities within the Western Interconnection; and (3) other non-substantive changes.

NERC’s filed petition was noticed on October 30, 2020, with interventions, comments, and protests due on or before November 27, 2020. No interventions, comments or protest 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 (2020), 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 (2020).

Sincerely,

Andrew Dodge, Director
Office of Electric Reliability

173 FERC ¶ 61,277
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: James P. Danly, Chairman;
Neil Chatterjee and Richard Glick.

North American Electric Reliability Corporation

Docket No. RR20-5-000

ORDER CONDITIONALLY APPROVING REVISED *PRO FORMA* DELEGATION
AGREEMENT AND REVISED DELEGATION AGREEMENTS WITH REGIONAL
ENTITIES

(Issued December 30, 2020)

1. On June 29, 2020, North American Electric Reliability Corporation (NERC) and the six Regional Entities¹ jointly petitioned the Commission to approve: (1) a revised *pro forma* Delegation Agreement; and (2) revised Delegation Agreements between NERC and each of the six Regional Entities. The currently-effective Delegation Agreements between NERC and each Regional Entity expire on December 31, 2020. NERC proposes that the revised Delegation Agreements become effective January 1, 2021.²

2. In this order, we conditionally approve the agreements in the Joint Petition to become effective January 1, 2021. As discussed below, we direct NERC and the Regional Entities to modify the revised *pro forma* Delegation Agreement and revised Delegation Agreements and submit a compliance filing to address these modifications within 120 days of the date of this order.

¹ The six Regional Entities are: Midwest Reliability Organization (MRO); Northeast Power Coordinating Council, Inc. (NPCC); ReliabilityFirst Corporation (ReliabilityFirst); SERC Reliability Corporation (SERC); Texas Reliability Entity (TRE); and Western Electricity Coordinating Council (WECC).

² *North American Electric Reliability Corporation, et al*, Petition for Approval of The Revised Pro Forma Regional Delegation Agreement And Revised Regional Entity Regional Delegation Agreement (June 29, 2020) (Joint Petition).

I. Background

3. On February 3, 2006, the Commission issued Order No. 672³ to implement the requirements of section 215 of the Federal Power Act (FPA) governing electric reliability.⁴ In July 2006, the Commission, pursuant to section 215 of the FPA, certified NERC as the Electric Reliability Organization (ERO).⁵ The Commission conditionally accepted NERC's proposal to delegate certain ERO functions to its designated Regional Entities. In addition, the Commission conditionally accepted NERC's proposed *pro forma* Delegation Agreement, and directed NERC to specify in its Rules of Procedure various due process procedures for its enforcement proceedings and initial hearings that the ERO and Regional Entities are to follow.⁶

4. On November 29, 2006, NERC submitted a compliance filing consisting of a Uniform Compliance Monitoring and Enforcement Program (CMEP) and a revised *pro forma* Delegation Agreement providing for the delegation of certain ERO functions and duties to Regional Entities. On the same date, NERC also submitted for Commission review and approval unexecuted Delegation Agreements between NERC and the proposed Regional Entities that, consistent with Order No. 672, 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.⁷ Further, the Delegation Agreements addressed: (1) regional Reliability Standards development; (2) registration of entities that must comply with Reliability Standards; and (3) other services supporting NERC's functions, including reliability assessments, event analysis, and training and education. The Commission accepted the *pro forma* Delegation Agreements and NERC's uniform

³ *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

⁴ 16 U.S.C. § 824o (2018).

⁵ *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 clarification and reh'g*, 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

⁶ ERO Certification Order, 116 FERC ¶ 61,062 at P 476.

⁷ Order No. 672, 114 FERC ¶ 61,104 at P 654.

CMEP including the CMEP Hearing Procedures, and the executed Delegation Agreements.⁸

5. On June 9, 2010, as supplemented on June 17, 2010, NERC filed a petition for the Commission to approve revisions to NERC's Rules of Procedure, the *pro forma* Delegation Agreement, Delegation Agreements between NERC and the Regional Entities, and bylaws of Florida Reliability Coordinating Council and MRO. On October 21, 2010, the Commission conditionally approved NERC's petition and directed NERC to submit a compliance filing.⁹ NERC submitted a compliance filing, and the Commission accepted the compliance filing on October 7, 2011.¹⁰

6. On June 26, 2015, NERC filed a petition requesting the Commission to approve revisions to NERC's Rules of Procedure, the *pro forma* Delegation Agreement and Delegation Agreements between NERC and the Regional Entities. On November 2, 2015, the Commission conditionally approved NERC's petition and directed NERC to submit a compliance filing.¹¹ NERC submitted a compliance filing, and the Commission accepted the compliance filing on March 23, 2016.

II. Joint Petition

7. In their June 29, 2020 Joint Petition, NERC and the Regional Entities propose revisions to the *pro forma* Delegation Agreement and its attachments, and the Delegation Agreements with the six Regional Entities. NERC requests that the Commission approve its proposals effective January 1, 2021.¹²

⁸ See *North American Electric Reliability Corp.*, 119 FERC ¶ 61,060 (2007) (accepting the *pro forma* Delegation Agreements and uniform CMEP); *Delegation Agreement Between the North American Electric Reliability Corp. and the Texas Regional Entity, a division of ERCOT*, 119 FERC ¶ 61,232 (2007) (accepting executed delegation agreements).

⁹ *North American Electric Reliability Corp.*, 133 FERC ¶ 61,061 (2010), *reh'g denied*, 134 FERC ¶ 61,179 (2011) (2010 Delegation Agreement Order).

¹⁰ *North American Electric Reliability Corp.*, 137 FERC ¶ 61,028 (2011). The Commission has accepted further modifications to some Delegation Agreements since October 7, 2011.

¹¹ *North American Electric Reliability Corp.*, 153 FERC ¶ 61,135 (2015).

¹² Joint Petition at 3.

8. NERC states that the proposed revisions to the *pro forma* Delegation Agreements reflect the evolution of NERC over the past five years, as NERC and the Regional Entities strengthen their activities and relationships under section 215 of the FPA.¹³ NERC submits that the governance structure of each Regional Entity ensures they perform their oversight role and delegated activities with adequate independence.¹⁴

9. NERC states that over the past five years, NERC, in consultation with the Regional Entities, has taken steps to further strengthen its commitment to independent governance. NERC explains that while section 215 of the FPA and Commission regulations permit each Regional Entity to be governed by an independent board, a balanced stakeholder board or a combination thereof (a “hybrid board”), the proposed revisions reflect NERC’s determination and the Regional Entities’ agreement that independent and hybrid boards provide greater independence than stakeholder boards, particularly with respect to oversight of the compliance and enforcement responsibilities of Regional Entities.¹⁵ Accordingly, section 2(a)(i) of the *pro forma* Delegation Agreement have been amended to remove the reference to balanced stakeholder board.¹⁶

10. NERC also proposes a new provision within section 2(a)(ii) of the *pro forma* Delegation Agreement stating that each Regional Entity executing the Delegation Agreement commits to maintaining a governing board with a sufficient number of independent members to perform certain oversight obligations related to governing a Regional Entity. NERC states that these obligations include: (1) nominating independent board members; (2) compensating the chief executive officer; (3) implementing the compliance monitoring and enforcement program; (4) retaining fair and reasonable compensation for independent board members; and (5) retaining appropriate conflict of interest and recusal policies for board members and staff alike.¹⁷

11. NERC also states that the proposed revisions include modifications to sections 4 and 9(j) of the *pro forma* Delegation Agreement to remove language previously

¹³ *Id.* at 2.

¹⁴ *Id.* at 3.

¹⁵ *Id.*

¹⁶ *Id.* at 8.

¹⁷ *Id.* at 8-9.

necessary to address Regional Entities performing functions of registered entities because there are no longer Regional Entities that perform such functions.¹⁸

12. NERC proposes to replace the existing maps of the Regional Entities' boundaries (Exhibit A) with descriptions of their geographic boundaries because the precision of the current maps varies across Regional Entities and may inadvertently provide misleading information. NERC argues that removing the maps will eliminate the need to amend the Delegation Agreements if a registered entity is transferred from one Regional Entity to another.¹⁹ Accordingly, NERC proposes to revise the recitals and sections 1(c) and 2(iv) of the *pro forma* Delegation Agreement to no longer reference the geographic boundaries "identified" in Exhibit A, but to reference the boundaries "described" in Exhibit A.²⁰ Each Regional Entity will be responsible for the enforcement of the Reliability Standards within its geographic boundaries described in Exhibit A.²¹

13. NERC proposes to modify section 6(e) of the *pro forma* Delegation Agreement to prohibit stakeholder representatives from leading a Regional Entity board compliance committee.²² NERC explains that the role of a compliance committee is to assist with oversight of Regional Entity decision-making within its compliance monitoring and enforcement program implementation. NERC states that to the extent that there is a compliance committee of a Regional Entity board, it should consist of a majority of independent board members and be chaired by an independent board member.²³

14. Further, NERC is amending section 12(b) of the *pro forma* Delegation Agreement to clarify that the Delegation Agreements may be terminated prior to the stated five-year term if the terminating party provides written notice to terminate no later than one year prior to the then-effective expiration of the term.²⁴

¹⁸ *Id.* at 9-10.

¹⁹ *Id.* at 7-8.

²⁰ *Id.*

²¹ *See Id.*, Attachment 1, Amended and Restated *Pro Forma* Regional Delegation Agreement, Clean Version, Section 2(iv) at 4.

²² *Id.* at 9.

²³ *Id.* at 9-10.

²⁴ *Id.* at 10.

15. In addition to the changes to the *pro forma* Delegation Agreement, NERC also outlined amendments to the Delegation Agreements with specific Regional Entities. Section 2(a)(i) of the MRO Delegation Agreement has been amended to reflect that MRO is governed by a hybrid board, and Exhibit D – Compliance Monitoring and Enforcement Program has been modified to reflect MRO’s adoption of the ERO Enterprise Consolidated Hearing Process as provided in the NERC Rules of Procedure. MRO may modify its selection of hearing process by notifying NERC six months prior to the decision becoming effective.²⁵

16. NERC states that section 2(a)(i) of the NPCC Delegation Agreement has been amended to reflect that NPCC is governed by a hybrid board, and Exhibit D – Compliance Monitoring and Enforcement Program has been modified to reflect NPCC’s adoption of the ERO Enterprise Consolidated Hearing Process as provided in the NERC Rules or Procedure. NERC notes that, consistent with the NERC Rules of Procedure and NPCC bylaws, NPCC may modify its selection of hearing process by notifying NERC six months prior to the decision becoming effective. NERC states that NPCC’s compliance committee is not a board committee but is comprised of NPCC technical expert members. NPCC also modified Exhibit A to remove potential compliance monitoring and enforcement activities outside of the NPCC region.²⁶

17. NERC states that section 2(a)(i) of the ReliabilityFirst Delegation Agreement has been amended to reflect that ReliabilityFirst is governed by a hybrid board, and Exhibit D – Compliance Monitoring and Enforcement Program has been modified to reflect ReliabilityFirst’s adoption of the ERO Enterprise Consolidated Hearing Process as provided in the NERC Rules of Procedure. ReliabilityFirst may modify its selection of hearing process by notifying NERC six months prior to the decision becoming effective.²⁷

18. NERC states that section 2(a)(i) of the SERC Delegation Agreement has been amended to reflect that SERC is governed by a hybrid board, and Exhibit D – Compliance Monitoring and Enforcement Program has been modified to reflect SERC’s adoption of the ERO Enterprise Consolidated Hearing Process as provided in the NERC Rules of Procedure. SERC may modify its selection of hearing process by notifying NERC six months prior to the decision becoming effective. SERC also

²⁵ *Id.* at 10-11.

²⁶ *Id.* at 11-12.

²⁷ *Id.* at 12.

modified Exhibit A to remove potential compliance monitoring and enforcement activities outside of the SERC region.²⁸

19. NERC states that section 2(a)(i) of the Texas RE Delegation Agreement has been amended to reflect that Texas RE is governed by a hybrid board, and updates Exhibit E – Funding to reflect current accounting, time record, and expense management for statutory and non-statutory activities.²⁹

20. NERC states that Exhibit D – Compliance Monitoring and Enforcement Program of the WECC Delegation Agreement has been modified to remove prior references to the Compliance Hearing Body in order to reflect WECC’s adoption of the ERO Enterprise Consolidated Hearing Process as provided in the NERC Rules of Procedure. NERC also explains that Exhibit E – Funding of the WECC Delegation Agreement has been revised to eliminate registered-entity-related functions from the scope of its statutory Situation Awareness activities.³⁰

21. NERC and the Regional Entities request the Commission approve the revised *pro forma* Delegation Agreement and the revised Delegation Agreements for each of the six Regional Entities, effective January 1, 2021, replacing the currently-effective Delegation Agreements that expire on December 31, 2020.³¹

III. Notice and Responsive Pleadings

22. Notice of NERC’s filing was published in the *Federal Register*, 85 Fed. Reg. 41,027 (July 8, 2020), with interventions and protests due before July 20, 2020. None were filed.

IV. Discussion

23. Except as otherwise described below, we approve the proposed *pro forma* Delegation Agreement and the revised Delegation Agreements between NERC and each of the six Regional Entities. As indicated in the Joint Petition, the revised *pro forma* Delegation Agreement and revised Delegation Agreements are the product of

²⁸ *Id.* at 12-13.

²⁹ *Id.* at 13.

³⁰ *Id.*

³¹ *Id.* at 4-5.

negotiations between NERC and each of the six Regional Entities, reflecting learned experiences operating under section 215 of the FPA and prior Delegation Agreements.

24. In approving the *pro forma* Delegation Agreements to become effective January 1, 2021, we also identify areas of concern and, where necessary to provide greater uniformity and clarity, direct modifications to the *pro forma* and individual Delegation Agreements, as discussed below. These modifications must be implemented by NERC and the Regional Entities in a filing to be made within 120 days from the date of this order.³²

A. Changes to Description of Geographic Boundaries

1. Joint Petition

25. The Joint Petition explains that the *pro forma* Delegation Agreement and each Delegation Agreement between NERC and each of the individual Regional Entities have been amended to clarify that Exhibit A (Regional Boundaries) reflects a description, not a map, of the Regional Entity's geographic boundaries.

2. Commission Determination

26. We agree with NERC that describing the boundaries of each of the Regional Entities instead of using a map is more accurate and precise. We also agree that amending the Delegation Agreements to replace the term "identified" with the term "described" when referencing the geographic boundaries relays a more accurate depiction of Exhibit A.

27. However, while the proposed *pro forma* Delegation Agreement updates the recitals and section 1(c) by replacing the term "identified" with "described," we note that this revision was not applied consistently throughout the *pro forma* Delegation Agreement or the revised individual Delegation Agreements. For instance, section 4(c) of the *pro forma* Delegation Agreement still states "[for] Cross-Border Regional Entities, the authority delegated by this agreement shall extend only to the portion of the region *identified* in Exhibit A" (emphasis added). Similarly, the individual Delegation Agreements between NERC and each of the Regional Entities do not reflect the change from "identified" to "described" in sections 1(c) or 4(c).

28. This revision should be applied consistently throughout the *pro forma* Delegation Agreement and individual Delegation Agreements between NERC and each of the

³² See 16 U.S.C. § 824o(b)(1) and (e)(5). Section 215 of the FPA provides that Regional Entities are subject to the Commission's jurisdiction and responsible for compliance with a Commission order affecting Regional Entities.

Regional Entities. Therefore, we direct NERC and the Regional Entities to make the necessary conforming changes.

B. Revisions to Exhibit D

1. Joint Petition

29. NERC states that apart from Texas RE, which will continue to use its Regional Hearing Process, each Regional Entity has adopted the Consolidated Hearing Process as provided in the NERC Rules of Procedure. Accordingly, the proposed revisions to Exhibit D, section 2 (Regional Hearing of Compliance Matters) of the Delegation Agreements of MRO, NPCC, ReliabilityFirst, and SERC specifically indicate the Regional Entities' adoption of the Consolidated Hearing Process, and state that consistent with the NERC Rules of Procedure and the bylaws of the individual Regional Entities, the Regional Entity may modify its selection of hearing process by notifying NERC six months prior to the decision becoming effective.

30. NERC has indicated in its transmittal letter that WECC has also adopted the Consolidated Hearing Process.³³ Accordingly, the WECC Delegation Agreement proposes to remove prior references to WECC's previous Compliance Hearing Body from Exhibit D, section 2. However, the revisions do not specifically indicate that WECC has adopted the Consolidated Hearing Process or provide language indicating that, consistent with the NERC Rules of Procedure, WECC may modify its selection of hearing process by giving NERC six months prior notice. The WECC Delegation Agreement states:

WECC, to the extent required in the Rules of Procedure, shall establish and maintain a hearing body with authority to conduct and render decisions in compliance hearings in which a Registered Entity may contest a finding of alleged violation, proposed penalty or sanction, or a proposed mitigation plan, which shall be either WECC's board, a committee of the board, a balanced compliance panel reporting directly to WECC's board or an independent hearing panel.

To the extent required in the Rules of Procedure, WECC shall conduct all compliance hearings in which a Registered Entity may contest a finding of alleged violation, proposed penalty or sanction, proposed Mitigation Plan, or a proposed Remedial Action Directive, in accordance with Attachment 2, Hearing Procedures, to the NERC Compliance Monitoring and Enforcement Program, subject to the following deviations, if any: None.

³³ Joint Petition at 13.

2. Commission Determination

31. Section 215(e)(4)(C) of the FPA requires that the Delegation Agreements between NERC and the Regional Entities promote effective and efficient administration of Bulk-Power System reliability.³⁴ This is achieved by implementing Delegation Agreements that include unambiguous language that makes clear the intent of the included provisions. We find that the proposed revisions to Exhibit D, section 2 of the WECC Delegation Agreement do not meet this standard because the section is not specific enough to indicate which hearing process WECC has selected in accordance with the NERC Rules of Procedure and could cause confusion as to which hearing process applies to registered entities. Therefore, we direct NERC to revise Exhibit D, section 2 of the WECC Delegation Agreement to clearly indicate that WECC has selected the Consolidated Hearing Process in accordance with the NERC Rules of Procedure and to submit the amended WECC Delegation Agreement in the compliance filing.

32. Additionally, we note that section 403.15 of the NERC Rules of Procedure states that a Regional Entity may modify its selection of hearing process by giving notice to NERC six months prior to such modification becoming effective. We also note that NERC proposes to revise the Delegation Agreements of MRO, NPCC, ReliabilityFirst, and SERC to include this provision in Exhibit D, section 2 of these Delegation Agreements. Notwithstanding the addition of this provision in the Delegation Agreements, it is our expectation that, if a Regional Entity modifies its selection of a hearing process, NERC will amend the Delegation Agreements and file such amendments with the Commission. This will ensure that the Delegation Agreements promote effective and efficient administration of the Bulk-Power System reliability by promoting transparency in the hearing process selection of each of the Regional Entities.

The Commission orders:

(A) NERC's revised *pro forma* Delegation Agreement and revised Delegation Agreements with the six Regional Entities are hereby conditionally approved to become effective January 1, 2021, as discussed in the body of this order.

(B) NERC and the Regional Entities are hereby directed to submit a compliance filing within 120 days of the date of this order to revise the *pro forma* Delegation Agreement, as discussed in the body of this order.

(C) NERC and the Regional Entities are hereby directed to include in its compliance filing, to be submitted within 120 days of the date of this order, revised

³⁴ 16 U.S.C. § 824o(e)(4)(c).

Docket No. RR20-5-000

- 11 -

individual Delegation Agreements with each Regional Entity reflecting the changes to the *pro forma* Delegation Agreement directed herein.

By the Commission. Commissioner Clements is not participating.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

Document Content(s)

RR20-5-000.DOCX.....1

174 FERC ¶ 61,031
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 39

[Docket No. RM21-12-000]

Revisions to Regulations on Electric Reliability Organization Performance Assessments

(Issued January 19, 2021)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to amend the Commission's regulations to require the Commission-certified Electric Reliability Organization to submit assessments of its performance every three years instead of the current period of every five years. The Commission also proposes to add to the Commission's regulations a requirement for the Electric Reliability Organization to include in its performance assessment a detailed discussion of any areas of the Electric Reliability Organization's responsibilities and activities, or a Regional Entity's delegated functions, beyond those required by the Commission's regulations, that the Commission has identified at least 90 days prior to the expected performance assessment submission date. Finally, the Commission proposes formalizing the method for the Electric Reliability Organization and Regional Entities to receive and respond to recommendations by the users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the Electric Reliability Organization's operations, activities, oversight and procedures.

DATES: Comments are due **INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

ADDRESSES: Comments, identified by docket number, may be filed electronically at <http://www.ferc.gov> in acceptable native applications and print-to-PDF, but not in scanned or picture format. For those unable to file electronically, comments may be filed by mail to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, N.E., Washington, D.C. 20426. Hand-delivered comments must be delivered to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852. The Comment Procedures Section of this document contains more detailed filing procedures.

FOR FURTHER INFORMATION CONTACT:

Leigh Anne Faugust (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-6396

SUPPLEMENTARY INFORMATION:

174 FERC ¶ 61,031
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Revisions to Regulations on Electric Reliability
Organization Performance Assessments

Docket No. RM21-12-000

NOTICE OF PROPOSED RULEMAKING

(Issued January 19, 2021)

1. Pursuant to section 215 of the Federal Power Act (FPA),¹ the Commission proposes to amend section 39.3(c) of the Commission's regulations to require the Commission-certified Electric Reliability Organization (ERO) to submit assessments of its performance every three years instead of the current period of every five years.² We believe that the proposed amendment will provide better continuity in our review of the ERO's operations, activities, oversight, procedures, and evaluation of the effectiveness of each Regional Entity in the performance of delegated functions. We also believe the proposed shorter performance assessment cycle will provide an opportunity to identify potential improvements with regards to ERO performance in a more timely fashion, allow for changes to be made in a more timely manner, and improve the efficiency of the overall performance assessment process.

¹ 16 U.S.C. 824o.

² 18 CFR 39.3(c).

2. Also, pursuant to section 215 of the FPA, we propose to add subsection (iv) to section 39.3(c)(1) of the Commission's regulations to require the Commission-certified ERO to include in its performance assessments a detailed discussion of any areas of the ERO's responsibilities and activities, or the Regional Entities' delegated functions, beyond those required by section 39.3(c)(1)(i), (ii), and (iii), that the Commission identifies for inclusion at least 90 days prior to the expected performance assessment submission date.

3. Finally, we propose to amend section 39.3(c)(1)(ii) of the Commission's regulations to require the ERO to solicit via a formal public comment period recommendations by the users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the ERO's operations, activities, oversight and procedures.

I. Background

A. Section 215 of the FPA

4. Section 215 of the FPA requires the Commission to issue regulations that, among other things, provide for the certification of an entity as the ERO if it meets certain criteria.³ Specifically, FPA section 215(c) establishes that an ERO candidate must have

³ 16 U.S.C. 824o; (on July 20, 2006, the Commission certified NERC as the ERO for the continental United States under FPA section 215(c)). *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 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).

the ability to develop and enforce mandatory Reliability Standards that provide for an adequate level of reliability of the Bulk-Power System.⁴ 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.

5. 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.

B. Order No. 672

6. On February 3, 2006, the Commission issued Order No. 672, which amended the Commission's regulations to implement the requirements of FPA section 215.⁵ In Order

⁴ *Id.* section 824o(c).

⁵ *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability*

No. 672, the Commission interpreted section 215 of the FPA to require the ERO to comply with the certification criteria in section 215(c) of the FPA on a continuous basis.⁶ Further, the Commission mandated that the ERO submit periodic assessments of its performance that “affirmatively demonstrate to the Commission that [the ERO] 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.”⁷

7. In Order No. 672, the Commission also said that the performance assessments should employ regular and systematic measurement and reporting of the ERO’s performance. The specific requirements for the performance assessments are set out in the Commission’s regulations in section 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. Section 39.3(c)(1) of the Commission’s regulations specify that the ERO should include in its performance assessment: (1) an explanation of how it satisfies the requirements of section 39.3 (b);⁸ (2) recommendations from stakeholders on improvement for the ERO and Regional Entities’ performance and the ERO’s and

Standards, Order No. 672, 71 FR 8662 (Feb. 17, 2006), 114 FERC ¶ 61,104, at P 186, *order on reh’g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

⁶ *Id.* PP 183, 187.

⁷ *Id.* P 186.

⁸ 18 CFR 39.3(c)(1)(i).

Regional Entities' response to those recommendations;⁹ and (3) an evaluation of the effectiveness of each Regional Entity's performance of delegated functions.¹⁰ Section 39.3(c)(2) of the Commission's regulations explain that the Commission will review the 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.¹¹

II. Discussion

8. Pursuant to section 215 of the FPA, we propose to amend section 39.3(c) of the Commission's regulations to require the Commission-certified ERO to submit assessments of its performance every three years instead of the current period of every five years.¹² We also propose to amend section 39.3(c)(1) to add a new requirement for the ERO to include in its performance assessment a detailed discussion of any areas of the EROs' responsibilities and activities, or the Regional Entity delegated functions, beyond those required by section 39.3(c)(1)(i), (ii), and (iii) that the Commission identifies at least 90 days prior to the expected performance assessment submission date. For example, a Commission-identified issue may be communicated to the ERO through a

⁹ 18 CFR 39.3(c)(1)(ii), (iii).

¹⁰ 18 CFR 39.3(c)(1)(iii).

¹¹ *Id.*

¹² 18 CFR 39.3(c).

Commission order or the Commission's delegated authority to the Director of the Office of Electric Reliability.¹³

9. While Order No. 672 established a five-year period for submitting ERO performance assessments following the initial three-year assessment, decreasing the periodicity to every three years would improve the ERO's accountability to the public, stakeholders, and the Commission. Our proposed reduction in the assessment period aligns with the ERO's own acknowledgement that it is "facing unprecedented, rapid change in the electric industry, which raises new challenges to and opportunities for the reliability and security of the Bulk Power System."¹⁴ We agree, and find that the Bulk-Power System is transitioning in myriad ways through innovation and technology at a pace unanticipated when the Commission originally established the five-year performance assessment period and identified topics for the ERO to include in those assessments.
10. The proposed three-year performance assessment cycle will enhance the Commission's oversight of the ERO and provide an opportunity to address issues arising with regard to ERO performance in a more timely fashion. We believe this will allow for

¹³ See e.g., 18 CFR 375.303 (a)(2)(v) ("The Commission authorizes the Director or the Director's designee to...[d]irect the Electric Reliability Organization, Regional Entities, or users, owners, and operators of the Bulk-Power System within the United States (not including Alaska and Hawaii) to provide such information as is necessary to implement Section 215 of the Federal Power Act. . . .").

¹⁴ *North American Electric Reliability Corp.*, Docket No. RR19-7-000, at 3 (July 22, 2019) (2019 Performance Assessment).

changes to be made in a more timely manner, and improve the efficiency of the overall performance assessment process. A three-year performance assessment aligns more closely with certain ongoing NERC activities, such as the triennial Reliability Standards and reliability guidelines reviews. Moreover, the reduced period between assessments will allow better continuity in the Commission's review of the ERO's operations, activities, oversight, procedures, and evaluation of the effectiveness of each Regional Entity in the performance of delegated functions. For example, a three-year period improves the likelihood that the NERC staff preparing the performance assessment, the Commission staff reviewing the assessment, and Commissioners would be familiar with the performance assessment process—thereby providing continuity and subject matter expertise. Three years also provides an earlier opportunity to address new and emerging areas of concern or recommendations for development identified by the Commission and stakeholders.

11. We believe that the proposed three-year performance cycle affords a reasonable amount of time between performance assessments. We note that this is the same three-year timeframe imposed in Order No. 672 on the initial performance assessment submitted by the ERO in 2010. The timing also aligns with the NERC's Rules of Procedure requirement of an independent audit of NERC's Compliance Monitoring

and Enforcement Program (CMEP) and Organization Registration and Certification Program.¹⁵

12. The ERO has existing internal processes used to assess its ongoing performance of its statutory responsibilities, and the Regional Entities' ongoing performance in their delegated activities.¹⁶ For example, NERC files itemized annual budgets for both its own activities and those of the Regional Entities, thereby tracking whether it "allocate[s] equitably reasonable dues, fees and charges among end users for all activities."¹⁷ The ERO uses a program alignment process to identify, prioritize, and resolve inconsistencies among the Regional Entities.¹⁸ The ERO also issues a stakeholder survey every other

¹⁵ See e.g., NERC, Rules of Procedure, sec. 406 ("NERC shall provide for an independent audit of its [CMEP] at least once every three years, or more frequently as determined by the Board. The audit shall be conducted by independent expert auditors as selected by the Board").

¹⁶ For example, pursuant to 18 CFR 39.3 (c)(1)(i), the ERO must include in its performance assessment an explanation of how its Reliability Standards program meet the requirements of section 39.3(b). NERC posts on its website the status of various Reliability Standards projects, and provides public access to all projects, including: Reliability Standards, Standard Authorization Requests, Periodic Reviews, and Interpretations. NERC, *Reliability Standards Under Development*, <https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx>. NERC has a formal oversight program for functions it has delegated to the Regional Entities. The programs include performance metrics that NERC uses to evaluate the Regional Entity performance from year to year, (i.e., more frequently than what would be necessary for a three-year performance assessment). 2019 Performance Assessment at 10.

¹⁷ 18 CFR 39.3(b)(2)(ii).

¹⁸ NERC, *ERO Enterprise Program Alignment Process*, <https://www.nerc.com/pa/comp/Pages/EROEnterProAlign.aspx>.

year to measure the effectiveness of NERC and the Regional Entities in executing program activities.¹⁹

13. Based on the examples described above, we believe the ERO should be able to use these existing processes to provide a self-assessment to the Commission on a three-year basis rather than every five years without imposing an undue burden on the ERO. NERC could leverage the existing tracking mechanisms discussed above, as well as the findings of its required three-year independent audit, its internal audit department, ongoing quarterly and annual assessments of its CMEP and Organization Registration and Certification Program,²⁰ and the processes that lead to NERC's annual filings of the business plan and budgets (and those of the Regional Entities),²¹ all of which NERC already uses to regularly report on its and the Regional Entities' activities. For these reasons, we believe a reduction of time from a five-year cycle to a three-year cycle will not impose an undue burden for NERC, the Regional Entities, registered entities, or other interested stakeholders.

¹⁹ As required by 18 CFR 39.3(c)(1)(ii), the ERO's performance assessment must address "the effectiveness of each Regional Entity, recommendations by the [ERO], users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the Regional Entity's performance of delegated functions."

²⁰ See e.g., NERC, *Compliance Monitoring and Enforcement Program Quarterly Report*, (Nov. 4, 2020), <https://www.nerc.com/pa/comp/CE/ReportsDL/Q3%202020%20Quarterly%20CMEP%20Report.pdf>.

²¹ See e.g., NERC, 2021 Business Plan and Budget Preparation Schedule, (2020), <https://www.nerc.com/gov/bot/FINANCE/Hidden%20Documents/2021%20BPB%20Preparation%20Schedule.pdf>.

14. Next, based on the last three performance assessments NERC has submitted to the Commission as the ERO, where the Commission has directed NERC to submit additional information on further compliance, we propose to revise the Commission's regulations governing what an ERO must include in its performance assessment. Specifically, we propose to require that the Commission-certified ERO include in its performance assessments a detailed discussion of any areas of the ERO's activities and functions, or the Regional Entities' delegated functions, beyond those set forth in section 39.3(c)(1)(i), (ii), and (iii), that the Commission identifies for inclusion at least 90 days prior to the expected performance assessment submission date.²² Identifying specific areas of interest in a formal and timely manner prior to NERC's submission of the Performance Assessment may likely result in efficiencies. For example, identifying areas of interest NERC should address in the filing may reduce the need for the Commission to issue data requests or require informational filings afterwards. We believe the additional information NERC will provide in response to the identified areas of interest will enable the Commission to more efficiently review the performance of the ERO's activities and functions, as well as oversight of the Regional Entities' delegated functions. We also believe 90 days prior to the submission of each performance assessment provides NERC adequate time to address any Commission-identified topics in its performance

²² As noted above, a Commission-identified issue may be communicated to the ERO through a Commission order or the Commission's delegated authority to the Director of the Office of Electric Reliability.

assessment, but we seek comment on whether a different period of time may be more appropriate.

15. Finally, we propose to add a formal requirement for a public comment period to solicit 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. The intent of the comment period is to inform the content of the ERO's draft performance assessment. We anticipate that the ERO would meet the proposed requirement by issuing notice of a public comment period on its website specifically requesting that interested parties identify areas of improvement. We envision the solicitation of comments would be issued separately and prior to the posting of the draft performance assessment. The posting should be independent of other recurring stakeholder surveys that may have a more limited audience. The ERO would then include the submitted comments, and the ERO's responses to such comments, with its performance assessment filing.

16. We believe that the proposed amendments to our regulations will improve our oversight of the ERO. The proposal will better enable the Commission to determine that the ERO is satisfying the statutory and regulatory criteria continuously,²³ and provide the opportunity for more timely Commission and stakeholder feedback or direction to the ERO should issues arise. Further, consistent with Order No. 672, the shorter cycle for the

²³ Order No. 672 interprets the FPA to require that the ERO to comply with the certification criteria on an ongoing basis, and that a violation of a certification criterion constitutes a violation of the FPA. Order No. 672, 114 FERC ¶ 61,104 at P 184.

ERO performance assessment will provide more timely Commission oversight to assure that the ERO is “not only maintaining but improving the quality of its activities and those of the Regional Entities to which it has delegated such activities.”²⁴ We seek comments from NERC and other interested entities on this proposal, including on the burden of this proposal.

III. Information Collection Statement

17. This NOPR proposes to amend the Commission’s regulations to require the Commission-certified ERO to submit assessments of its performance every three years instead of the current period of every five years. It also proposes to require the Commission-certified ERO to include in its performance assessments a detailed discussion of any areas of the ERO’s responsibilities and activities, or the Regional Entities’ delegated functions, beyond those required by § 39.3(c)(1)(i), (ii), and (iii), that the Commission identifies for inclusion at least 90 days prior to the expected performance assessment submission date. Finally, this NOPR proposes to formalize the ERO’s solicitation of recommendations via a formal public comment period from 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.

²⁴ Order No. 672, 114 FERC ¶ 61,104 at P 186.

18. The Paperwork Reduction Act (PRA)²⁵ requires each federal agency to seek and obtain approval by the Office of Management and Budget (OMB) before undertaking a collection of information (including reporting, record keeping, and public disclosure requirements) directed to ten or more persons or contained in a rule of general applicability. OMB regulations²⁶ require approval of certain information collection requirements contemplated by proposed rules (including deletion, revision, or implementation of new requirements). Upon approval of a collection of information, OMB will assign an OMB control number and an expiration date. Respondents subject to the filing requirements of this proposed rule will not be penalized for failing to respond to the collection of information unless the collection of information displays a valid OMB control number.

19. The information collection in this NOPR is FERC-725, “Certification of Electric Reliability Organization.” The OMB Control Number is 1902-0225. As required by the PRA, the collection of information that would be revised in this proposed rule is being submitted to OMB for review under 44 U.S.C. 3507(d).

20. The Commission solicits comments on the Commission’s need for the proposed revision of the information collection, 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

²⁵ 44 U.S.C. 3501-3521.

²⁶ 5 CFR Part 1320.

respondents' burden, including the use of automated information techniques. All burden estimates are discussed in this NOPR and in the Paperwork Reduction Act supporting statement.

21. Interested persons may submit questions about this information collection by contacting Ellen Brown, Office of the Executive Director, at DataClearance@ferc.gov, or (202) 502-8663. Please send comments concerning the collection of information and the associated burden estimates to: Office of Information and Regulatory Affairs, Office of Management and Budget [Attention: Federal Energy Regulatory Commission Desk Officer]. Due to security concerns, comments should be sent directly to www.reginfo.gov/public/do/PRAMain. Comments submitted to OMB should be sent within 60 days of publication of this notice in the Federal Register and refer to FERC-725 and OMB Control No. 1902-0225.

22. Please submit to the Commission copies of comments concerning the collection of information and the associated burden estimates (identified by Docket No. RM21-12-000) by any of the following methods:

- eFiling at Commission's Web Site: <http://www.ferc.gov/docs-filing/efiling.asp>;
- U.S. Postal Service Mail: Persons unable to file electronically may mail similar pleadings to the Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426; or
- Effective July 1, 2020, filings not submitted via eFiling or the U.S. Postal Service may be delivered to: Federal Energy Regulatory Commission, c/o

Health and Human Services, 12225 Wilkins Avenue, Rockville, Maryland 20852.

23. The following discussion describes and analyzes the existing collection of information associated with 18 CFR 39.3(c) (FERC-725, OMB Control Number 1902-0225), as it would be modified by this proposed rule.

- *Necessity of the Information:* The information collected from the ERO or Regional Entities under the requirements of FERC-725 is used by the Commission to implement the statutory provisions of section 215 of the FPA and implemented by the Commission in accordance with 18 CFR part 39.
- *Public Reporting Burden:* The NOPR would result in program changes in the “Self-Assessment” information activities in FERC-725 due to the proposed requirement to submit self-assessments every 3 years. At present, self-assessments are required every 5 years.

24. The annualized number of responses for each self-assessment would be revised from 0.2 per year to 0.33 per year. As shown below, RM21-12-000 would result in a total of 2.31 responses for self-assessments annually. The Commission has also reduced the number of Regional Entities from seven to six.

25. The Commission calculates the average annual burden and cost²⁷ in accordance with data from the Bureau of Labor Statistics. For hourly cost (for wages and benefits),

²⁷ The hourly cost estimates are based on wage data from the Bureau of Labor Statistics for May 2019 (BLS, *Occupational Employment Statistics* (May 2019), https://www.bls.gov/oes/current/naics2_22.htm) and benefits data for September 2020

we estimate that 70 percent of the time is spent by Electrical Engineers (code 17-2071, at \$66.90/hr.), 20 percent of the time is spent by Legal (code 23-0000, at \$143.68/hr.), and 10 percent by Office and Administrative Support (code 43-0000, at \$41.34/hr.). The weighted hourly cost (for wages and benefits) is \$79.70.

A. Type of Respondent	B. Type of Response	C. No. of Respondents	D. No. of Responses Per Respondent	E. Total No. of Responses (Col. C x Col. D)	F. Average Burden Hours & Cost (\$) per Response (rounded)	G. Estimated Total Annual Burden Hrs. & Cost (\$) (rounded) (Col. E x Col. F)
Electric Reliability Organization	Self- Assessment	1	0.33	0.33	4,160 hrs.; \$331,552	1,373 hrs.; \$109,412
Regional Entities	Self- Assessment	6	0.33	1.98	4,160 hrs.; \$331,552	8,237 hrs.; \$656,473
Total Burden Hrs. and Cost		7		2.31		9,610 hrs.; \$765,885

IV. Environmental Analysis

26. 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.²⁸ 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

(BLS, *Employer Costs for Employee Compensation Summary* (Dec. 17, 2020), <https://www.bls.gov/news.release/ecec.nr0.htm>).

²⁸ *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

not substantially change the effect of the regulations being amended.²⁹ The actions proposed here fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Certification

27. The Regulatory Flexibility Act of 1980 (RFA)³⁰ generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.

28. By only proposing to direct NERC, the Commission-certified ERO, to increase the periodicity of its performance assessment submission and address identified topics, this NOPR will not have a significant or substantial impact on entities other than NERC. The ERO develops and files with the Commission for approval Reliability Standards affecting the Bulk-Power System, which represents: (a) a total electricity demand of 830 gigawatts (830,000 megawatts) and (b) more than \$1 trillion worth of assets. Therefore, the Commission certifies that this NOPR will not have a significant economic impact on a substantial number of small entities.

VI. Comment Procedures

29. 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 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

²⁹ 18 CFR 380.4(a)(2)(ii).

³⁰ 5 U.S.C 601-612.

Comments must refer to Docket No. RM21-12-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

30. 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.

31. Commenters that are not able to file comments electronically must submit an original of their comments either by mail through the United States Postal Service to: the Secretary of the Commission, Federal Energy Regulatory Commission, 888 First Street N.E., Washington, DC, 20426,³¹ or by any other method of delivery, including hand delivery, to the Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852.³²

32. 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.

³¹ 18 CFR 385.2001(a)(1)(i).

³² 18 CFR 385.2001(a)(1)(ii).

VII. Document Availability

33. 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>). At this time, the Commission has suspended access to the Commission's Public Reference Room due to the President's March 13, 2020 proclamation declaring a National Emergency concerning the Novel Coronavirus Disease (COVID-19).

34. 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.

35. 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 39

Administrative practice and procedure

Electric power

Penalties

Reporting and recordkeeping requirements

By direction of the Commission. Commissioners Chatterjee and Glick are concurring with a joint separate statement attached.

(S E A L)

Kimberly D. Bose,
Secretary.

In consideration of the foregoing, the Commission proposes to amend part 39, chapter I, title 18, *Code of Federal Regulations*, as follows:

The authority citation for part 250 continues to read as follows:

Authority: [16 U.S.C. 824o](#).

1. Amend § 39.3 by revising paragraph (c) to read as follows.

§ 39.3 Electric Reliability Organization certification

(c) The Electric Reliability Organization shall submit an assessment of its performance three years from the date of certification by the Commission, and every three years thereafter. After receipt of the assessment, the Commission will establish a proceeding with opportunity for public comment in which it will review the performance of the Electric Reliability Organization.

2. Amend § 39.3 by adding new paragraph (iv) is as follows.

§ 39.3 Electric Reliability Organization certification

(iv) a detailed discussion of any areas of the Electric Reliability Organizations responsibilities and activities, or the Regional Entity delegated functions, beyond those required by § 39.3(c)(1)(i), (ii), and (iii) that the Commission has identified. The Commission will inform the Electric Reliability Organization of any additional performance areas to include at least 90 days prior to the expected performance assessment submission date.

3. Amend § 39.3 by revising paragraph (c) to read as follows.

§ 39.3 Electric Reliability Organization certification

(ii) Recommendations, as solicited by the Electric Reliability Organization via a noticed public comment period, by Regional Entities, users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the Electric Reliability Organization's operations, activities, oversight and procedures, and the Electric Reliability Organization's response to such recommendations...

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Revisions to Regulations on Electric Reliability
Organization Performance Assessments

Docket No. RM21-12-000

(Issued January 19, 2021)

CHATTERJEE, Commissioner, and GLICK, Commissioner, *concurring*:

We support this notice of proposed rulemaking (NOPR), which explores potential improvements to the existing framework for the North American Electric Reliability Corporation, the Commission-certified Electric Reliability Organization (ERO), to submit assessments of its performance. Given the important and increasingly complex role the ERO plays in ensuring the reliability of the Bulk Power System, we urge interested parties to submit comments on the proposed reforms. To that end, while we encourage comments on the potential benefits of these proposed reforms, we also encourage interested parties to provide comments on the potential burdens the proposed reforms may impose on the ERO and its Regional Entities.

For these reasons, we respectfully concur.

Neil Chatterjee
Commissioner

Richard Glick
Commissioner

173 FERC ¶ 61,243
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: James Danly, Chairman;
Neil Chatterjee, and Richard Glick.

Virtualization and Cloud Computing Services

Docket No. RM20-8-000

ORDER DIRECTING INFORMATIONAL FILING

(Issued December 17, 2020)

1. On February 20, 2020, the Commission issued a Notice of Inquiry (NOI) seeking comments on the potential benefits and risks associated with the use of virtualization and cloud computing services in association with bulk electric system (BES) operations.¹ The Commission also sought comments on whether barriers exist in the Commission-approved Critical Infrastructure Protection (CIP) Reliability Standards that impede the voluntary adoption of virtualization or cloud computing services.

2. As discussed below, there is general agreement in the NOI comments that the voluntary use of virtualization and cloud computing could provide significant benefits to users, owners and operators of the Bulk-Power System so long as the risks associated with these technologies are carefully addressed. Without pre-judging their outcomes, we believe that the two North American Electric Reliability Corporation (NERC) standard drafting projects addressing virtualization and data storage (i.e., BES Cyber System Information (BCSI)) with third parties will facilitate the use of virtualization and cloud

¹ *Virtualization and Cloud Computing Services*, 170 FERC ¶ 61,110 (2020) (Notice of Inquiry). Virtualization is the process of creating virtual, as opposed to physical, versions of computer hardware to minimize the amount of physical computer hardware resources required to perform various functions. *Id.* P 4. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. *Id.* P 7.

computing by clarifying their compliance treatment in the CIP Reliability Standards.² We recognize, however, that some commenters advocate for even greater use of virtualization and cloud computing than what is currently being considered by the NERC standard drafting teams. Accordingly, as discussed below, we direct NERC to make an informational filing that considers the feasibility of modifying the CIP Reliability Standards to facilitate the voluntary use of virtualization and cloud computing for purposes beyond data storage (i.e., to perform BES reliability operating services), as well as the status and schedule for any plans to modify the standards by NERC.³ We direct NERC to submit this informational filing by January 1, 2022.

I. Background

A. Notice of Inquiry

3. The NOI sought comment on four topics: (A) scope of potential use of virtualization and cloud computing services; (B) potential benefits and risks associated with virtualization and cloud computing services; (C) potential impediments to adopting virtualization and cloud computing services; and (D) potential use of new and emerging technologies in the current CIP Reliability Standards framework.⁴ The NOI indicated that the Commission would use information in the comments to determine whether it would be appropriate, pursuant to section 215(d)(5) of the Federal Power Act, to direct NERC to develop modifications to the CIP Reliability Standards to facilitate the voluntary adoption of virtualization and cloud computing services by registered entities.⁵

4. Concurrently with the NOI, the Commission issued an order (Scheduling Order) directing NERC to submit a schedule and quarterly updates for NERC Project 2016-02 and Project 2019-02 (collectively, NERC Projects).⁶

² NERC Project 2016-02 (Modifications to CIP Standards) and Project 2019-02 (BES Cyber System Information Access Management).

³ See Notice of Inquiry, 170 FERC ¶ 61,110 at P 16 (identifying certain reliability operating services).

⁴ *Id.* at P 14.

⁵ *Id.* at P 3; 16 U.S.C. § 824o(d)(5).

⁶ *North American Electric Reliability Corp.*, 170 FERC ¶ 61,109 (2020).

B. Comments and Reply Comments

5. The Commission received 26 comments and three reply comments, generally supporting the voluntary use of virtualization and cloud computing services provided the risks associated with these technologies are mitigated.

6. NERC supports the use of virtualization, including to perform the BES reliability operating services identified in the NOI, if appropriate controls are implemented to mitigate the potential risks.⁷ NERC cautions that virtualization may create risks to data security and increases the complexity of systems by adding layers of technology, which can make it more difficult to spot anomalies or unusual events happening on the network and the virtual machine. NERC states, however, that it has observed registered entities using virtualization and successfully mitigating known risks. In addition, NERC states that it supports the use of cloud computing for storage of BCSI. NERC identifies four risks related to cloud computing generally: (1) data security; (2) quality of service and resiliency; (3) ERO Enterprise oversight; and (4) infrastructure and operations. However, NERC contends that these risks can be appropriately mitigated in the context of third-party data storage. Moreover, NERC observes that some responsible entities already use cloud computing services for data storage, including BCSI storage.⁸

7. Other commenters generally agree with NERC's view that virtualization and data storage, including BCSI storage, with third parties can be implemented while addressing the risks associated with those technologies. The comments also support providing more clarity in the CIP Reliability Standards to mitigate compliance risk. MISO Transmission Owners state, for example, that there are no significant technical challenges to implementing virtualization, but there is compliance risk.⁹ Public Power Trade Associations note that some of its members have encountered auditors who do not understand virtualization and therefore recommend against its use or are unwilling to confirm that virtualized configurations would be compliant with the CIP Reliability

⁷ BES reliability operating services include dynamic response to BES conditions, balancing load and generation, controlling frequency (real power), controlling voltage (reactive power), managing constraints, monitoring and control, restoration of BES, situational awareness, and inter-entity real-time coordination and communication. Notice of Inquiry, 170 FERC ¶ 61,110 at P 16.

⁸ NERC Comments at 5, 6, 8-12.

⁹ MISO Transmission Owners Comments at 17.

Standards.¹⁰ ISO/RTO Council (IRC) states that many registered entities have not fully deployed virtualization technologies due to the potential compliance risks.¹¹ The National Rural Electric Cooperative Association (NRECA) maintains that a compliance challenge may arise from the need for a registered entity to provide evidence to show how it is meeting the CIP Reliability Standards.¹²

8. The NOI comments contain less consensus on performing BES reliability operating services in the cloud at this time. NERC indicates that it could support the use of cloud computing for purposes other than BCSI storage, such as BES reliability operating services, if appropriate protections are adopted to mitigate the risks and vulnerabilities.¹³ While NERC contends that the same risks associated with BCSI storage also apply to the performance of BES reliability operating services in the cloud, NERC's comments suggest that these risks are more acute for BES reliability operating services. NERC also indicates that it has not seen registered entities use cloud computing for BES reliability operating services, but NERC acknowledges that "certain support services are increasingly being offered through cloud computing services."¹⁴

9. NRECA, Public Power Trade Associations, Edison Electric Institute (EEI), IRC and the Canadian Electricity Association (CEA), among others, identify benefits to adopting cloud computing technology for BES reliability operating services. Public Power Trade Associations state that potentially all BES reliability operating services that are system-based could be moved to the cloud and that cloud services offer technological advancements, sophistication and cost savings, including security features that may not otherwise be available to all utilities, particularly smaller entities.¹⁵ EEI explains that cloud services could eliminate system downtime and improve patching and user administration.¹⁶ NRECA states that cloud computing resources are more easily scalable to best fit the environment, allowing the entity to pay only for what is necessary

¹⁰ The American Public Power Association and the Large Public Power Council (collectively, Public Power Trade Associations) filed joint comments; Public Power Trade Associations Comments at 13.

¹¹ IRC Comments at 11.

¹² NRECA Comments at 15.

¹³ NERC Comments at 8-12.

¹⁴ *Id.* at 8.

¹⁵ Public Power Trade Associations Comments at 5.

¹⁶ EEI Comments at 13, 16.

and easily or rapidly expand capability based on changing demand. NRECA also states that the cloud potentially can provide improved security over what a smaller utility might be able to have in a non-cloud environment.¹⁷

10. MISO Transmission Owners and NRECA state that while BES reliability operating services could be implemented in a virtualized environment, the full range of services should not be implemented in the cloud.¹⁸ CEA states that it prefers that real-time BES operations be kept within the registered entity's direct control. Among the risks, CEA raises concerns about the potential consequences of cloud unavailability.¹⁹

C. NERC's Reliability Standard Projects Schedule

11. In response to the Scheduling Order, NERC filed an initial schedule on March 19, 2020 for the NERC Projects and three subsequent updates. In the most recent update filed on November 13, 2020, NERC indicates that it anticipates filing Reliability Standards resulting from the NERC Projects in December 2021.

12. NERC explains that the Project 2016-02 standard drafting team is considering modifications to five CIP Reliability Standards and their associated definitions,²⁰ as well as conforming changes to other Reliability Standards, to address permitted architecture and the security risks of virtualization technologies. In addition, NERC states that, because entities already use virtualized technologies on-premise or plan to implement them, NERC is preparing a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide that addresses virtualization on-premise (Virtualization CMEP Practice Guide) to provide direction to CMEP staff, including auditors, on audit and compliance assessment approaches under the currently-effective CIP Reliability Standards. NERC maintains that the Virtualization CMEP Practice Guide will provide clarity on how CMEP staff will verify compliance in light of virtualized technologies and highlight the

¹⁷ NRECA Comments at 9.

¹⁸ *Id.* at 5-6; MISO Transmission Owners at 13-14.

¹⁹ CEA Comments at 3,7.

²⁰ NERC November 13, 2020 Informational Filing at 3 (identifying Reliability Standards CIP-004-6 (Personnel & Training), CIP-005-6 (Electronic Security Perimeter(s)), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (System Security Management), and CIP-010-3 (Configuration Change Management and Vulnerability Assessments)).

types of information CMEP staff may review to assess compliance and reliability risk. NERC notes that it plans on issuing the Virtualization CMEP Practice Guide by February 2021.²¹

13. NERC maintains that Project 2019-02 includes proposed modifications to currently-enforceable Reliability Standards CIP-004-6 (Personnel and Training) and CIP-011-2 (Information Protection) and is intended to facilitate the use of third-party data storage and analysis systems by clarifying the minimum protections expected when a responsible entity utilizes these solutions.²²

II. Discussion

A. NERC Reliability Standard Projects

14. We support NERC's effort to reassess the CIP Reliability Standards to facilitate the adoption of virtualization and cloud computing and relieving registered entities of compliance uncertainties. However, consistent with the precept that the Reliability Standards are technology-neutral, virtualization and cloud computing should continue to be voluntary to allow registered entities to consider the deployment of these new technologies, their system needs, and applicable security requirements.²³

15. Based on these considerations, we support the completion of the NERC Projects based on the schedules provided in the November 13, 2020 Informational Filing, which target the filing of proposed Reliability Standards with the Commission in December 2021. We also support NERC's interim step to issue a Virtualization CMEP Practice Guide by February 2021. We believe that issuance of the Virtualization CMEP Practice Guide will provide more certainty to registered entities utilizing virtualization technologies on-premise and mitigate the compliance risk associated with their use. The anticipated proposed Reliability Standards coupled with NERC's Virtualization CMEP Practice Guide should provide a more comprehensive regulatory framework designed to ensure system reliability while facilitating the voluntary adoption of new technologies.

²¹ *Id.* at 4-5.

²² *Id.* at 5-6.

²³ *See, e.g., Reliability Standards for Geomagnetic Disturbances*, Order No. 779, 143 FERC ¶ 61,147, at P 81, *reh'g denied*, 144 FERC ¶ 61,113 (2013) (acknowledging that Reliability Standards should be technology neutral).

B. Virtualization and Cloud Computing for BES Reliability Operating Services and Other Uses

16. The NOI comments suggest that the use of cloud computing could be expanded for purposes other than BCSI storage, such as for performing BES reliability operating services. However, NERC and other commenters express concern with moving such functions to the cloud at present.

17. As with BCSI storage, cloud utilization for BES reliability operating services or other uses may offer benefits, including cost savings and enhanced security and resiliency features that may be otherwise unavailable to some registered entities, particularly smaller entities.²⁴ Despite these benefits, we agree with NERC that facilitating BES operations in the cloud should be carefully evaluated prior to developing new, or modifying existing, Reliability Standards. To ensure that such evaluation occurs, we direct NERC to begin a formal process to assess the feasibility of voluntarily conducting BES operations in the cloud in a secure manner and to make an informational filing by January 1, 2022 that evaluates potential modifications to the CIP Reliability Standards to facilitate expanded use of the cloud, including to perform BES operations. The informational filing should report on any new or future NERC standard drafting projects, their status and schedule.

18. The NOI comments discuss various aspects of expanded cloud usage, including ensuring quality of service (e.g., reliable communication networks), resiliency (e.g., registered entity reliance on one major cloud provider creating a single point of failure and registered entities' having adequate on-site back-up capability), and compliance oversight (e.g., creating compliance processes that accommodate the use of third-party cloud service providers, such as the Federal Risk and Authorization Management Program).

19. In developing the informational filing, NERC should consider the NOI comments, including the security objectives to mitigate risks by entities voluntarily using virtualization implemented off-premises and cloud computing; potential for the use of BES reliability operating services data and the storage or use of BCSI outside the registered entity's country; evaluation criteria for the selection of cloud service providers for use by the electric industry; allowing registered entities to conduct their own reliability risk assessments to determine what BES reliability operating services and other services can be securely performed in the cloud; and establishing a clear dividing line between the security responsibilities of the cloud service provider and the registered entity. NERC's informational filing should also consider whether establishing a new audit process, which could provide auditors access to cloud service providers' facilities,

²⁴ Public Power Trade Associations Comments at 5.

Docket No. RM20-8-000

- 8 -

is necessary to ensure that registered entities that elect to use cloud service providers are in compliance with all applicable CIP Reliability Standards.

The Commission orders:

NERC is directed to begin a formal process to assess the feasibility of voluntarily conducting BES operations in the cloud in a secure manner and to make an informational filing by January 1, 2022, as discussed in the body of this order.

By the Commission. Commissioner Clements is not participating.

(S E A L)

Kimberly D. Bose,
Secretary.

Document Content(s)

RM20-8-000.DOCX.....1

174 FERC ¶ 61,030
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: James P. Danly, Chairman;
Neil Chatterjee, Richard Glick,
Allison Clements, and Mark C. Christie.

North American Electric Reliability Corporation

Docket No. RR19-7-001

ORDER ON COMPLIANCE FILINGS

(Issued January 19, 2021)

On June 1, 2020 and September 28, 2020, the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted compliance filings in accordance with the Commission's order accepting NERC's 2019 Five-Year Performance Assessment.¹ In addition to providing the required information on its various programs, NERC requests Commission approval of its proposal to replace the audits contemplated in Appendix 4A of the NERC Rules of Procedure, and requests approval of modifications to its Rules of Procedure related to: (1) the Electricity Information Sharing and Analysis Center (E-ISAC) (section 1003); (2) Sanction Guidelines (Appendix 4B); and (3) Registration and Certification (section 500 and Appendices 2, 5A, 5B, and 5C).

We approve NERC's proposed modifications to its Rules of Procedure related to: (1) the E-ISAC (section 1003); (2) Sanction Guidelines (Appendix 4B); and (3) Registration and Certification (section 500 and Appendices 2, 5A, 5B, and 5C). However, for the reasons discussed below, the Commission denies NERC's proposal to replace its Appendix 4A audit process with an alternative program and directs NERC to submit completed reports on its audits of all six Regional Entities by June 30, 2023. We accept NERC's description of its Reliability Guidelines process, its explanation on E-ISAC operations, and its explanation of its All Points Bulletins (APBs) issuances; however, we direct NERC to submit a further compliance filing within 120 days of this order that: (1) further clarifies information sharing between NERC and the E-ISAC, including the gap analysis process that is currently under development; and (2) revises its Rules of Procedure to explicitly require that NERC must share all APBs with the Commission no later than at the time of issuance.

¹ *North American Electric Reliability Corp.*, 170 FERC ¶ 61,029, at PP 54, 59, 68, 70, and 72 (2020) (Performance Assessment Order).

I. Performance Assessment Order

Section 215(c) of the Federal Power Act (FPA) requires the ERO to develop and enforce mandatory Reliability Standards that provide for an adequate level of reliability of the Bulk-Power System.² Order No. 672 amended the Commission's regulations to implement the requirements of FPA section 215, and, among other things, requires the ERO to submit periodic assessments of its performance every five years.³ On July 22, 2019, NERC filed its Five-Year ERO Performance Assessment Report (2019 Performance Assessment) as required by Commission regulations.

On January 23, 2020, the Commission issued an order accepting NERC's 2019 Performance Assessment, finding that NERC continues to satisfy the statutory and regulatory criteria for certification as the ERO, and finding that the Regional Entities continue to satisfy applicable statutory and regulatory criteria. In addition, the Commission directed NERC to submit two compliance filings to: (1) provide additional information on NERC's oversight of the Regional Entities' Compliance Monitoring and Enforcement Program (CMEP) activities, the reliability guideline development process, the E-ISAC, and the development and issuance of APBs; and (2) make certain modifications to its Rules of Procedure regarding the E-ISAC, the NERC Sanction Guidelines, and the NERC Organization Certification Program.

With regard to NERC's oversight of the Regional Entities' CMEP activities, the Commission noted that, from 2011 through the end of 2018, NERC may not have performed comprehensive audits of the Regional Entities to assess their conformance to the NERC CMEP, as required by both NERC's Rules of Procedure and regional delegation agreements. In the Performance Assessment Order, the Commission directed NERC to submit the following:

(1) a definitive statement of whether NERC has performed any audits of the Regional Entities during the performance assessment period covering the scope of Appendix 4A, and if so, provide its audit reports in compliance with its Rules of Procedure; and (2) if it has not performed such audits, provide a plan to perform those audits within the next 18 months and going forward. If NERC would like to implement an alternative oversight process for the Regional Entities that it believes is as efficient and effective as the comprehensive [Appendix 4A] audits conducted every five years, then its

² 16 U.S.C. 824o(c).

³ *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, at P 186, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

compliance filing should include a detailed explanation of how its oversight process accomplishes the aims of Order No. 672.⁴

The Commission also directed NERC to provide additional detail regarding its NERC Reliability Guidelines, specifically: (1) its guidance development process; including how and when it evaluates the need to develop, approve, and post a guideline document; (2) the methodology and metrics NERC proposes to use to determine if that guidance document is addressing the risks that led to its development; and (3) how and at what interval NERC will evaluate whether components of guidance documents should be incorporated into the Reliability Standards.⁵

Regarding the E-ISAC, the Commission directed NERC to file additional information on: (1) how NERC receives information from the E-ISAC and how the E-ISAC determines what data to share with NERC; (2) once NERC receives such information, what NERC does with the information and how NERC determines whether such information is used to develop or inform the development of Reliability Standards; (3) the oversight role of the Member Executive Committee (an advisory group formed out of the Electricity Subsector Coordinating Council (ESCC)); (4) the development of E-ISAC's performance metrics and how they assist NERC in its oversight responsibility of the E-ISAC; and (5) the development and issuance of APBs.

With regard to the second compliance filing, the Commission directed NERC to propose updates to: (1) section 1003 of its Rules of Procedure to correct any inconsistencies, particularly regarding the ESCC, and to reflect current operational practices and oversight of the E-ISAC;⁶ (2) its Sanction Guidelines to provide more transparency as to how NERC and the Regional Entities apply the Base Penalty, Adjustment Factors and Non-Monetary Sanctions;⁷ and (3) to include in the certification process: (A) an updated scope section covering the tools and skills needed to perform the registered function; (B) the minimum criteria for certification, including verification that the entity's tools, personnel, facilities, and processes can fully support the function; and (C) a mechanism to reject the request for certification if the entity does not meet the requirements for certification. The Commission also directed NERC to consider whether

⁴ See e.g., Order No. 672, 114 FERC ¶ 61,104 at P 773.

⁵ Performance Assessment Order, 170 FERC ¶ 61,029 at P 59.

⁶ *Id.* P 74.

⁷ *Id.* P 81.

it should permit a conditional approval of an entity that does not meet the requirements for certification if it includes an approved mitigation plan.⁸

II. NERC's Compliance Filings

On June 1, 2020, NERC submitted its first compliance filing.⁹

On September 28, 2020, NERC submitted its second compliance filing.¹⁰

III. Notice of Filings and Responsive Pleadings

Notice of NERC's June Compliance Filing was issued on June 3, 2020, and published in the *Federal Register*, 85 Fed. Reg. 35,303 (June 9, 2020), with comments due on or before June 22, 2020. Public Citizen filed timely joint comments with the National Association of State Utility Consumer Advocates (NASUCA) (jointly, Consumer Advocates).¹¹

Notice of NERC's September Compliance Filing was issued on September 30, 2020, and published in the *Federal Register*, 85 Fed. Reg. 63,109 (Oct. 6, 2020) with comments due on or before October 19, 2020. No interventions or comments were filed.

IV. Discussion

We accept NERC's June Compliance Filing's discussion addressing Reliability Guidelines and the E-ISAC. However, we reject NERC's proposal to change its Rules of Procedure to remove the Appendix 4A audit requirements, combining them with sections

⁸ *Id.* P 86.

⁹ *North American Electric Reliability Corp.*, Compliance Filing in Response to the Order on the Five-Year Performance Assessment, Docket No. RR19-7-001 (June 1, 2020) (June Compliance Filing).

¹⁰ *North American Electric Reliability Corp.*, Second Compliance Filing of the North American Electric Reliability Corporation in Response to the Order on the Five-Year Performance Assessment, Docket No. RR19-7-001 (September 28, 2020) (September Compliance Filing).

¹¹ Consumer Advocates "suggest[] reforms to enhance representation for household consumers and strengthen governance." Consumer Advocates Comments at 1. We dismiss Consumer Advocates' comments as outside the scope of this proceeding, as they do not address whether the June Compliance Filing complies with the Commission's directives in the Performance Assessment Order.

406 and 506. We accept NERC's description of its Reliability Guidelines process and its explanation on E-ISAC operations. We accept NERC's September compliance filing and approve NERC's proposed modifications to its Rules of Procedure: (1) the E-ISAC (section 1003); (2) Sanction Guidelines (Appendix 4B); and (3) Registration and Certification (section 500 and Appendices 2, 5A, 5B, and 5C). In addition, we accept NERC's description of its APBs. However, as discussed below, we direct NERC to modify its Rules of Procedure to explicitly require NERC to share all APBs with the Commission no later than the time of issuance.

A. Periodic Regional Entity CMEP Audits

June Compliance Filing

In the June Compliance Filing, NERC states that it has completed two audits of the Regional Entities during the period and they were limited to the areas of the CMEP related to: (1) confidential information and conflict of interest procedures; and (2) internal controls evaluations of registered entities.¹² NERC included the audit report from the confidential information audit but not from the internal controls evaluations. NERC adds it completed two non-CMEP audits of the Regional Entities' event analysis processes and FPA section 215 accounting for non-statutory activities. NERC included the two non-CMEP audit reports with the non-public compliance filing.

Rather than providing a plan to complete Appendix 4A audits within an 18-month period, NERC elected to propose changes to its internal audit process. NERC describes modifications that it would make to its Rules of Procedure to implement the proposal. Specifically, NERC proposes to: (1) expand the scope of sections 406 and 506¹³ in the Rules of Procedure to encompass CMEP and Organization Registration and Certification Program (ORCP) activities; (2) clarify that sections 406 and 506 allow for participants from its Compliance and Certification Committee and applicable governmental authorities (e.g., the Commission); (3) delete the procedural and substantive requirements

¹² June Compliance Filing at 7.

¹³ Sections 406 and 506 address independent audits only of NERC. In section 406, NERC must provide for an independent audit (conducted by independent expert auditors as selected by the Board) of its CMEP at least once every three years, or more frequently as determined by the Board. The independent audit must meet the following minimum requirements and any other requirements established by the NERC Board: (1) effectiveness, i.e., section 406 requires the audit to "evaluate the success and effectiveness of the NERC [CMEP] in achieving its mission;" and (2) relationship, i.e., section 406 requires the audit to "evaluate the relationship between NERC and the Regional Entity [CMEPs] and the effectiveness of the programs in ensuring reliability."

of Appendix 4A; and (4) make conforming changes eliminating all references to Appendix 4A.

NERC's June Compliance Filing proposes that its internal audit department conduct audits of both NERC and the Regional Entities. Under NERC's proposal, NERC's internal auditors would evaluate not only NERC's CMEP and ORCP, but also NERC's relationship with the Regional Entities' CMEP programs. NERC proposes that its audits of the Regional Entities would examine what NERC calls the "regulatory programs" (i.e., CMEP, ORCP, and Bulk Electric System Exceptions) at least once every three years.¹⁴ These audits may, but would not be required to, use an independent auditor and would take place at NERC, without Appendix 4A's site visits.¹⁵ NERC explains that the audits would examine "shall statements" related to the regulatory programs and its internal audit department would "determine the specific scope of each audit in collaboration with any independent auditors and participating observers."¹⁶ NERC proposes submitting the resulting audit reports to the Commission after providing them to the NERC Board of Trustees.

NERC states that its proposal is consistent with the requirements of Order No. 672 because it provides for "(i) Audits within a defined frequency; (ii) Commission visibility into results (i.e., submission of audit reports); and (iii) Commission participation in any audit of Regional Entities."¹⁷ NERC explains it believes its proposal is more effective and efficient than a single five-year audit because including regulatory program audits within NERC's independent audit of CMEP and ORCP activities will "support a robust, independent, audit that is consistent with the intent in Order No. 672, while enhancing frequency of audits, increasing efficiency, and streamlining procedures."¹⁸

Commission Determination

While the Performance Assessment Order permitted NERC to propose an alternative oversight program for the Regional Entities, we find that NERC failed to demonstrate that its proposed alternative oversight program would accomplish the aims

¹⁴ June Compliance Filing at 9.

¹⁵ *Id.*

¹⁶ *Id.* at 10.

¹⁷ *Id.* at 9.

¹⁸ *Id.* at 11.

of Order No. 672.¹⁹ Although NERC's proposal provides for a defined audit frequency, submittal of audit reports to the Commission, and Commission staff participation, we find that it does not sufficiently assess the Regional Entities' compliance and performance.²⁰

The alternative proposal is insufficient in that it limits the scope of audits of the Regional Entities to evaluations of whether "shall statements" associated with the Rules of Procedure and the regional delegation agreements are met. Unlike in Appendix 4A, NERC does not propose any required scope or procedural rules, but instead explains that NERC internal audit will determine the scope of the audits. In addition, NERC's proposal effectively reduces the scope of the required audits and fails to consider that, in accordance with the existing Rules of Procedure, audits of Regional Entities must be qualitative reviews with the objective of ensuring consistency and fairness of the Regional Entities' CMEPs.

While NERC maintains that its proposed audit process would identify and evaluate compliance with "shall statements" in the NERC Rules of Procedure and other documents, NERC's description of its audit or oversight activities does not explain how NERC's alternative process considers risk in the determination of elements to review, the timing of audit activities, or how it would assess the quality of audited Regional Entities' performance. Moreover, NERC does not explain how its internal audit department will prioritize sections of the Rules of Procedure for audit, nor does it provide examples of past audits conducted pursuant to sections 406 and 506 to consider.

The aims of Order No. 672 include the mandate that the ERO "retains responsibility to ensure that a Regional Entity implements its enforcement program in a consistent manner"²¹ Appendix 4A satisfies the requirements of Order No. 672 by providing defined content and procedures for NERC audits of the Regional Entities' CMEPs. In lieu of Appendix 4A, NERC proposes that a single entity within NERC, referred to as "internal audit," will: (1) audit the success and effectiveness of NERC's [CMEP] (which under current NERC Rules of Procedure section 406 is performed by an independent auditor); (2) "evaluate the relationship between NERC and the Regional Entity [CMEPs] and the effectiveness of the [Regional Entity CMEPs] in ensuring reliability;" and (3) evaluate the Regional Entities' CMEPs. In addition to the potential conflict of NERC evaluating its own CMEP and its relationship with the Regional Entities, a single audit evaluating NERC's and the Regional Entities' CMEPs at the same

¹⁹ See, e.g., Order No. 672, 114 FERC ¶ 61,104 at P 773.

²⁰ *Id.*

²¹ *Id.* P 486.

time would appear to erode the ERO/Regional Entity structure required by Order No. 672.

For these reasons, we reject NERC's proposal to change its Rules of Procedure to remove the Appendix 4A audit requirements, combining them with sections 406 and 506. We direct NERC to complete Regional Entity audits consistent with section 402 and Appendix 4A and provide the resulting audit reports to the Commission by June 30, 2023. Consistent with Appendix 4A, Commission staff shall be given the opportunity to participate in the audits as observers.

B. Reliability Guidelines

June Compliance Filing

NERC's June Compliance Filing presents a new framework to formalize how NERC will address known and emerging risks and evaluate what tool(s) or sequence of tool(s) are most appropriate to address each risk. NERC describes this six-step framework as: (1) risk identification; (2) risk prioritization; (3) mitigation identification and evaluation; (4) deployment; (5) measurement of success; and (6) monitoring.²² NERC explains that it will use steps one through three to determine whether a potential risk is best addressed through a voluntary Reliability Guideline, a Reliability Standard, or some other method. NERC provides examples of methods to identify risks and factors to prioritize risks for mitigation. NERC explains that mitigation activities could include Reliability Standards, Reliability Guidelines, Technical Engagements, Reliability Assessments, Alerts, and other potential mechanisms. NERC examines the likelihood and impact of reliability risks, dividing all risks into four categories: high likelihood-high impact; high likelihood-low impact; low likelihood-high impact; and low likelihood-low impact. NERC provides example tools for how it would mitigate risks that fall into these four categories, with Reliability Standards as a potential tool for only the high impact categories and Reliability Guidelines as a potential tool for all but high impact-high likelihood.²³

NERC explains that its Reliability and Security Technical Committee (RSTC) Charter has combined the procedures for developing Reliability Guidelines under its areas of responsibility. NERC explains that all Reliability Guidelines go through public comment and RSTC approval before being posted on NERC's website. After a Guideline is posted, the RSTC would assess industry's implementation and the effectiveness of the Guideline.

²² June Compliance Filing at 13.

²³ *Id.* at 17.

NERC explains that its RSTC will assess the implementation and effectiveness of all new or revised Reliability Guidelines two years after receiving RSTC approval.²⁴ NERC intends to apply a methodology to evaluate whether a Reliability Guideline is sufficient to address a risk to reliability. The methodology would assess metrics surrounding how the Bulk-Power System performed before and after a Reliability Guideline was posted, based on long-term and seasonal reliability assessments. Finally, NERC stated that it would develop metrics specific to each Reliability Guideline through its design, triennial review, and any resulting revision.²⁵ NERC's RSTC has the initial responsibility of working through the six-step framework and evaluating the performance of Reliability Guidelines, which NERC would then evaluate after receiving the RSTC's recommendations.

Commission Determination

The June Compliance Filing is the first time NERC has identified a framework for evaluating voluntary Reliability Guidelines. We find that NERC's June Compliance Filing, including its commitment to conduct triennial reviews of its Reliability Guidelines,²⁶ addresses our directives by providing a high level plan for evaluating whether a Reliability Guideline is appropriate for a given risk and assessing the efficacy of each Reliability Guideline to determine whether there is a need for further updates or modifications or whether they should be converted into Reliability Standards. In that vein, we clarify our expectation that NERC will use its voluntary Reliability Guidelines as a tool to support its Reliability Standards or in situations where it lacks sufficient technical support to draft a technically correct Reliability Standard, but not as a substitute for Reliability Standards. NERC's statutory authority as the ERO is to develop and enforce mandatory Reliability Standards.

C. E-ISAC Data-Sharing, Oversight, and Performance Metrics

June Compliance Filing

NERC's June Compliance Filing clarifies that the E-ISAC can share sanitized (i.e., with entity-specific details redacted) information with NERC, and by extension, NERC's

²⁴ *Id.* at 18.

²⁵ *Id.* at 19.

²⁶ We expect NERC to inform the Commission on the results of its first triennial review, either upon completion of the review or as part of its next Performance Assessment filing.

Standards department.²⁷ NERC describes its intent to enhance the coordination between the E-ISAC and the NERC Standards department by increasing knowledge exchange between subject matter experts in E-ISAC and the ERO Enterprise, initiating quarterly meetings between the E-ISAC and Standards department personnel to discuss E-ISAC information, subject to the Code of Conduct restrictions. NERC adds that the E-ISAC may share with the NERC Standards department any mandatory reports submitted to the E-ISAC in accordance with the Critical Infrastructure Protection Reliability Standard CIP-008 (Cyber Security – Incident Reporting and Response Planning). NERC also commits to establishing a process whereby Standards personnel and ERO Enterprise subject matter experts for CIP Reliability Standards review E-ISAC information, subject to the Code of Conduct restrictions, perform reliability gap analysis.

NERC clarifies that the Members Executive Committee (MEC) has influence on the E-ISAC as an advisory body only and does not possess any approval power. NERC explains that the MEC may propose or endorse action for the E-ISAC, but that the NERC Board of Trustees is ultimately responsible for approving those actions—and NERC management for implementing them. NERC states that “[t]he ESCC’s and the MEC’s expectation is that NERC management and the NERC Board give due consideration to the MEC’s proposals and endorsements within the context of fulfilling its legal and fiduciary obligations.”²⁸

NERC further explains in its filing that the scope of the E-ISAC’s metrics measure the E-ISAC performance against the three pillars of the E-ISAC Long-Term Strategic Plan and its effectiveness in carrying out the key activities underlying the plan: (1) engagement; (2) information sharing; and (3) analysis. NERC also lays out plans to evolve its E-ISAC performance metrics over time to be a mix of quantitative and qualitative measurements as it progresses, and data sources mature.

Commission Determination

We find that NERC has responded to the directives in the Performance Assessment Order and therefore accept NERC’s clarification and additional detail.²⁹ Representing 37.9 percent of NERC’s FPA section 215 funding for the 2021 fiscal year,³⁰ the E-ISAC fills an important role in ensuring the ongoing security of the Bulk-Power System. Through

²⁷ *Id.* at 20-22.

²⁸ *Id.* at 27.

²⁹ We address the directive concerning APBs in a later section.

³⁰ See NERC 2021 Budget Filing, Attachment 2 at 1, North American Electric Reliability Corp., Docket RR20-6-000 (Aug. 24, 2020).

its activities, it is poised to discover emerging threats that could be addressed, in part, through new or modified Reliability Standards. We accept NERC's clarifications, NERC's stated intent to improve coordination between the E-ISAC and NERC, and NERC's commitment to create a process to perform a gap analysis for the Reliability Standards. However, because we are unsure how the E-ISAC Code of Conduct and its limitations prohibiting information sharing with NERC Reliability Standards personnel may restrict this activity, we will require NERC to submit an additional compliance filing within 120 days of the date of this order that outlines this process.

D. Rules of Procedure Revisions Regarding E-ISAC

September Compliance Filing

NERC proposes changes to its Infrastructure Security Program in section 1003 of the NERC Rules of Procedure. The proposed modifications clarify that NERC operates the E-ISAC on behalf of the electricity sector. NERC also defines the ESCC as serving as the "primary security communications channel for the electricity sector," explaining that it "enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents."³¹ The proposed modifications add that the E-ISAC is required to coordinate with the ESCC in addition to other sectors and councils.³²

Commission Determination

The Commission directed NERC to propose updates to section 1003 of its Rules of Procedure to correct any inconsistencies, particularly regarding the ESCC, and to reflect current operational practices and oversight of the E-ISAC.³³ We find NERC met the requirements of the Commission directive and we approve the proposed modifications to NERC's Rules of Procedure, section 1003.

E. Rules of Procedure Revisions Regarding Sanction Guidelines

September Compliance Filing

NERC's proposed revisions detail how it and the Regional Entities determine the base penalty amount within the range based on Violation Risk Factor and Violation Severity Level and other documented factors. NERC identifies what aggravating and mitigating factors can affect the monetary penalty and describes the potential ranges for

³¹ September Compliance Filing at 261.

³² *Id.* at 16.

³³ Performance Assessment Order, 170 FERC ¶ 61,029 at P 74.

each factor, and whether or how non-monetary penalties will be considered in reaching the final monetary penalty amount. NERC also addresses how it and the Regional Entities calculate a single penalty for multiple violations by a single entity, consider the violator's financial ability to pay the penalty so that no penalty is inconsequential to the violator to whom it is assessed, and how to assess a penalty when dealing with multiple subsidiaries of a parent corporation that commit the same violations. NERC states that other revisions include conforming changes and clarifications to accurately reflect the current practices of NERC and the Regional Entities in the development of monetary and non-monetary penalties.

Commission Determination

In the Performance Assessment Order, the Commission directed NERC to provide more transparency in its Sanction Guidelines as to how NERC and the Regional Entities apply the Base Penalty, Adjustment Factors, and Non-Monetary Sanctions.³⁴ We find NERC has provided more clarity and transparency into the penalty assessment process, and thus we accept the proposed modifications to the NERC Sanction Guidelines.

F. Rules of Procedure Revisions Regarding NERC Organization Registration and Certification Program

September Compliance Filing

NERC explains that it is adding new subsections to the existing certification process section, which includes how NERC addresses the Commission's directives on Certification. NERC proposes modifications to its registration and certification procedures in its Rules of Procedure section 500 and Appendices 2, 5A, 5B, and 5C. To address the requirement to include an updated scope section, NERC added that certification activities would "assess the processes, procedures, tools, and training"³⁵ that the entities use in performing their functions. To address the Commission's directive for a mechanism to reject a request for certification, NERC added that a Regional Entity may reject an application if the entity fails to meet registry criteria or is unable to comply with the relevant NERC Reliability Standards for its functions.³⁶ NERC also added a section to require a timeline with specific milestones for the Certification process. To address the Commission's directive regarding conditional approvals, NERC added that it can issue a conditional certification to allow an entity to begin operation for a function for which it is not fully approved if an interim transition is warranted. The conditional

³⁴ *Id.* P 81.

³⁵ September Compliance Filing at 13.

³⁶ *Id.* at 14.

acceptance is based on the entity's ability to manage the function with limited risk while completing an implementation plan to address the identified shortcomings. This conditional certification requires review of the impacts of an entity being delayed or failing to be certified and requires an implementation plan to address delayed or failed certification to prevent gaps in reliability coverage.³⁷

Commission Determination

The Performance Assessment Order directed NERC to include in the certification process: (1) an updated scope section covering the tools and skills needed to perform the registered function; (2) the minimum criteria for certification, including verification that the entity's tools, personnel, facilities, and processes can fully support the function; and (3) a mechanism to reject the request for certification if the entity does not meet the requirements for certification. The Commission also directed NERC to consider whether it should permit a conditional approval of an entity that does not meet the requirements for certification if it includes an approved mitigation plan.³⁸ We find that NERC met the requirements of the Commission directive and we approve the proposed modifications to its Rules of Procedure section 500 and Appendices 2, 5A, 5B, and 5C.

G. Critical Broadcast Program and All Points Bulletins

September Compliance Filing

NERC's September Compliance Filing explains the purpose of the Critical Broadcast Program (CBP) is to "provide for the rapid dissemination of critical security information to electricity sector asset owners and operators as security threats and attacks develop, and critical, time-sensitive security information becomes available."³⁹ NERC explains that because cyber and physical security threats and attacks develop quickly, the CBP provides an "established approach for sharing time-sensitive information with electricity sector asset owners and operators to help them prevent an imminent cyber or physical attack on the grid, reduce the scope of a successful attack, or implement ongoing measures to defend against an attack."⁴⁰ A CBP communication could take the form of a conference call or webinar with relevant entities or the issuance of a written document, referred to as an APB, posted on the E-ISAC portal or disseminated through other

³⁷ *Id.* at 15.

³⁸ Performance Assessment Order, 170 FERC ¶ 61,029 at P 86.

³⁹ September Compliance Filing at 29.

⁴⁰ *Id.*

channels “as deemed appropriate” by the E-ISAC given the facts and circumstances presented.

NERC explains the process for activating the CBP involves: (1) a threshold for activation such as “reports from governmental partners, E-ISAC members, and private-sector partners” or disclosure of cyber vulnerabilities; (2) approving activation, while any E-ISAC staff can start the process of developing an APB, the NERC officer responsible for the E-ISAC makes the final approval—and the NERC President must be informed prior to activation; (3) a targeted audience based on the nature and target of the threat or attack (e.g., all or select groups of asset owners, government, cross-sector partners, executive level or cyber experts, etc.); (4) methods of communication, as NERC explains: “[w]hen activating the CBP, the E-ISAC, as time permits, also works with its governmental partners and the ESCC to share critical information and enhance situational awareness;” and (5) timing of communication where the E-ISAC then determines when to communicate, adding that the E-ISAC aims to communicate within six hours of its awareness of a developing security threat.⁴¹

NERC explains that the CBP “works in conjunction with, and complements other information sharing mechanisms, such as the NERC Alert process.”⁴² It differentiates the two because it considers the NERC Alert process to be a more “deliberative and collaborative process for developing a more detailed analysis of security risks and mitigation approaches.”⁴³ NERC adds that issuing an APB does not exclude also developing a NERC Alert or other communication. NERC points to four factors it uses to determine whether to activate the CBP versus a NERC Alert process: (1) the time-sensitive nature of the information; (2) the need for flexibility in the method of communications; (3) the audience; and (4) the need for an industry response.⁴⁴

Commission Determination

We find NERC’s September Compliance Filing addresses the Commission directive to clarify its APB processes. However, to ensure the Commission is properly informed of any cyber and physical security threats and attacks communicated through APBs, we will require NERC to modify its Rules of Procedure to explicitly require NERC to share all

⁴¹ *Id.* at 30.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.* at 31.

APBs with the Commission no later than the time of issuance.⁴⁵ We will require NERC to file such revisions to its Rules of Procedures within 120 days of the date of this order. Due to the time sensitivity of APBs, we will not require at this time that NERC provide advance notice to the Commission prior to issuance; however, when possible, we expect NERC to share APBs with the Commission prior to their issuance.

The Commission orders:

(A) The Commission hereby accepts NERC's compliance filings, as discussed in the body of this order.

(B) The Commission hereby denies NERC's request to modify its Appendix 4A audit requirements, as discussed in the body of this order.

(C) The Commission hereby approves NERC's Rules of Procedure modifications, as discussed in the body of this order.

(D) The Commission hereby directs NERC to submit its Appendix 4A audit reports by June 30, 2023, as discussed in the body of this order.

(E) The Commission hereby directs NERC to submit a compliance filing within 120 days, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

⁴⁵ See 16 U.S.C 824o (f) ("The Commission, upon its own motion or complaint, may propose a change to the rules of the ERO . . .").

Document Content(s)

RR19-7-001.DOCX.....1

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

SUNSHINE ACT MEETING NOTICE

January 12, 2021

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: January 19, 2021
10:00 A.M.

PLACE: Open to the public via audio Webcast only.¹

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://ferc.capitolconnection.org/> using the eLibrary link.

¹ Join FERC online to listen live at <http://ferc.capitolconnection.org/>.

1074th - MEETING

OPEN MEETING

January 19, 2021

10:00 AM

Item No.	Docket No.	Company

ADMINISTRATIVE

A-1	AD21-1-000	Agency Administrative Matters
A-2	AD21-2-000	Customer Matters, Reliability, Security and Market Operations

ELECTRIC

E-1	RM20-10-000	Electric Transmission Incentives Policy Under Section 219 of the Federal Power Act
E-2	Omitted	
E-3	EL21-7-000	Cricket Valley Energy Center, LLC and Empire Generating Company, LLC v. New York Independent System Operator, Inc.
E-4	RR19-7-001	North American Electric Reliability Corporation
E-5	RM21-12-000	Revisions to Regulations on Electric Reliability Organization Performance Assessments
E-6	RM21-11-000	Accounting and Reporting Treatment of Certain Renewable Energy Assets
E-7	AC20-103-000	Locke Lord LLP
E-8	ER20-3040-001 ER20-3042-000 ER20-3042-001 ER20-3043-001 ER20-3044-001 ER20-3045-001 (not consolidated)	Southwestern Electric Power Company
E-9	Omitted	
E-10	Omitted	
E-11	Omitted	
E-12	Omitted	
E-13	Omitted	

E-14	Omitted	
E-15	AD20-9-000	Hybrid Resources
E-16	Omitted	
E-17	EL20-30-001	Indiana Municipal Power Agency, and City of Lawrenceburg, Indiana v. PJM Interconnection, L.L.C., American Electric Power Service Corp., and Lawrenceburg Power, LLC
	EL20-56-001	PJM Interconnection, L.L.C.
E-18	Omitted	
E-19	EL16-49-004	Calpine Corporation, Dynegy Inc., Eastern Generation, LLC, Homer City Generation, L.P., NRG Power Marketing LLC, GenOn Energy Management, LLC, Carroll County Energy LLC, C.P. Crane LLC, Essential Power, LLC, Essential Power OPP, LLC, Essential Power Rock Springs, LLC, Lakewood Cogeneration, L.P., GDF SUEZ Energy Marketing NA, Inc., Oregon Clean Energy, LLC, and Panda Power Generation Infrastructure Fund, LLC v. PJM Interconnection, L.L.C.
	ER18-1314-007	PJM Interconnection, L.L.C.
	ER18-1314-008	
	EL18-178-004	
	(Consolidated)	
E-20	EL16-49-006	Calpine Corporation, Dynegy Inc., Eastern Generation, LLC, Homer City Generation, L.P., NRG Power Marketing LLC, GenOn Energy Management, LLC, Carroll County Energy LLC, C.P. Crane LLC, Essential Power, LLC, Essential Power OPP, LLC, Essential Power Rock Springs, LLC, Lakewood Cogeneration, L.P., GDF SUEZ Energy Marketing NA, Inc., Oregon Clean Energy, LLC, and Panda Power Generation Infrastructure Fund, LLC v. PJM Interconnection, L.L.C.
	EL18-178-006	PJM Interconnection, L.L.C.
	ER18-1314-010	

Gas

G-1	RP21-38-000	Northern Border Pipeline Company
G-2	Omitted	
G-3	RP21-216-000	Driftwood Holdings LLC and Driftwood LNG LLC
G-4	RP20-608-002	ANR Pipeline Company
G-5	Omitted	

HYDRO

H-1	RM21-9-000	Financial Assurance Measures for Hydroelectric Projects
H-2	Omitted	
H-3	P-2299-082 P-14581-002	Turlock Irrigation District and Modesto Irrigation District

H-4	Omitted	
H-5	Omitted	
H-6	Omitted	
H-7	P-2660-030	Woodland Pulp LLC
H-8	P-2486-088	Wisconsin Electric Power Company

Certificates

C-1	RM21-10-000	Categorical Exclusions under the National Environmental Policy Act
C-2	CP20-466-000	New Fortress Energy LLC
C-3	CP15-17-005	Sabal Trail Transmission, LLC
C-4	Omitted	
C-5	Omitted	
C-6	Omitted	
C-7	CP16-454-002	Rio Grande LNG, LLC
C-8	CP16-9-011	Algonquin Gas Transmission, LLC Maritimes & Northeast Pipeline, LLC
C-9	CP20-48-000	Iroquois Gas Transmission System, L.P.
C-10	CP20-47-000	PennEast Pipeline Company, LLC
C-11	CP21-12-000	Mountain Valley Pipeline, LLC
C-12	CP20-459-000	Golden Pass LNG Terminal LLC
C-13	CP16-10-000	Mountain Valley Pipeline, LLC
C-14	RM20-15-001	Limiting Authorizations to Proceed with Construction Activities Pending Rehearing
C-15	CP20-518-000	PennEast Pipeline Company, LLC
C-16	CP17-494-003 CP17-495-003	Pacific Connector Gas Pipeline, LP Jordan Cove Energy Project L.P.
C-17	Omitted	
C-18	CP17-40-005	Spire STL Pipeline LLC
C-19	CP16-10-008	Mountain Valley Pipeline, LLC

Kimberly D. Bose
Secretary

The public is invited to listen to the meeting live at <http://ferc.capitolconnection.org/>. Anyone with Internet access who desires to hear 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 audio webcast. The Capitol Connection provides technical support for this free audio webcast. It will also offer access to this event via phone bridge for a fee. If you have any questions, visit <http://ferc.capitolconnection.org/> or contact Shirley Al-Jarani at 703-993-3104.

January 2021

Commission Meeting Summaries

These are summaries of orders voted by the Federal Energy Regulatory Commission at its January 19, 2021 public meeting. The summaries are produced by FERC's Office of External Affairs and are intended to provide only a general synopsis of the orders. These summaries are not intended as a substitute for the Commission's official orders. To determine the specific actions and the Commission's reasoning, please consult the individual orders when they are posted to FERC's eLibrary found at www.ferc.gov.

E-4 & E-5 – Press Release

H-1 – Press Release

FERC seeks comment on a Notice of Inquiry

E-6, *Accounting and Recording Treatment of Certain Renewable Energy Assets*, Docket No. RM21-11-000. This Notice of Inquiry solicits comment on (1) whether the Commission should create new accounts for non-hydro renewable generating assets in the Uniform System of Accounts (USofA), (2) revisions to FERC Form No. 1 to reflect any such new accounts, (3) whether the Commission should codify the proper accounting treatment of renewable energy credits, and (4) the rate implications of these potential accounting and reporting changes.

FERC denies a filing

E-7, *Locke Lord LLP*, Docket No. AC20-103-000. The order denies Locke Lord's request for confirmation that the cost of specific wind and solar generating equipment can be properly booked to Uniform System of Accounts (USofA) Accounts 343, 344, and 345.

FERC directs submission of information on hybrid resource

E-15, *Technical Conference on Hybrid Resources*, Docket No. AD20-9-000. The order directs each Regional Transmission Organization (RTO) and Independent System Operator (ISO) to submit information related to hybrid resources. Specifically, we seek information in a report from each RTO/ISO regarding four hybrid resource issues: (1) terminology; (2) interconnection; (3) market participation; and (4) capacity valuation.

FERC addresses arguments raised on rehearing

E-17, *Indiana Municipal Power Agency v. PJM Interconnection, L.L.C.*, Docket No. EL20-30-001. The order modifies the discussion and sustains the result of the Commission's September 17, 2020 order in this proceeding, that granted, in part, and denied, in part, a petition for declaratory relief and complaint filed by Indiana Municipal Power Agency and the City of Lawrenceburg, Indiana against PJM, American Electric Power Service Corp., and Lawrenceburg Power, LLC concerning the station power self-supply monthly netting provision of the PJM Open Access Transmission Tariff.

FERC addresses a compliance filing

E-19, *Calpine Corporation v. PJM Interconnection, L.L.C.*, Docket No. EL16-49-004. The order accepts, in part, and rejects, in part, PJM's compliance filing in the Minimum Offer Price Rule Proceeding. The order finds most of PJM's filing is in compliance with the previous Compliance Order issued October 15, 2020 but rejects one provision added by PJM regarding the market seller offer cap that exceeds the directives of the underlying order. The order also denies the Market Monitor's request for clarification of the Compliance Order regarding replacement capacity and fixed resource requirement revenue.

FERC grants a retroactive waiver request

G-1, *Northern Border Pipeline Company*, Docket No. RP21-38-000. The order grants a retroactive waiver of Northern Border Pipeline Company's tariff and related Commission capacity release regulations to permit Northern Border to correct a rate that was erroneously applied in a temporary, pre-arranged capacity release that ran from November 2019 through March 2020.

FERC grants a prospective limited waiver

G-3, *Driftwood Holdings LLC and Driftwood LNG LLC*, Docket No. RP20-216-000. On November 13, 2020, Driftwood Holdings LLC (Driftwood Holdings) and Driftwood LNG LLC (Driftwood LNG) (jointly, Driftwood) filed a petition requesting a prospective limited waiver of the Commission's buy/sell prohibition and any relevant capacity release regulations and policies, as well as any other prospective waivers, to the extent necessary to enable Driftwood to purchase gas from potentially affiliated upstream suppliers that may be resold in foreign commerce to a different affiliate under a long-term contract for export as liquefied natural gas in foreign commerce. The order finds that good cause has been shown to grant, to the extent necessary, a prospective limited waiver of the Commission's buy/sell prohibition in the circumstances set forth by Driftwood.

FERC addresses arguments raised on rehearing

G-4, *ANR Pipeline Company*, Docket No., RP20-608-001. The order finds the Commission did not err in the August 31, 2020 order accepting ANR's proposed scheduling penalty during non-critical periods and revisions to its penalty waiver provisions. The order also grants a clarification requested by ANR and explains that ANR's swing percentage should be applied to those rate schedules that explicitly provide for a swing percentage, not to all rate schedules generally.

FERC denies petition for a declaratory order

H-3, *Turlock Irrigation District and Modesto Irrigation District*, Project Nos. 2299-082 and 14581-002. The order denies the Turlock Irrigation District and Modesto Irrigation District's October 2, 2020 petition for an order declaring that the California State Water Resources Control Board waived its authority under section 401(a)(1) of the Clean Water Act to issue water quality certifications for the Don Pedro and La Grange Hydroelectric projects.

FERC addresses arguments raised on rehearing

H-8, *Wisconsin Electric Power Company*, Project No. 2486-088. The order addresses requests for rehearing of the Commission's November 19, 2020 Order extending the license term for Wisconsin Electric Power Company's Pine Project No. 2486 so that the Pine Project's expiration date would align with the expiration date of 12 other projects located on the Upper Menominee River Basin, allowing the cumulative impacts of these projects to be assessed at the same time. The order modifies and sustains the result of the November 19, 2020 order, explaining that extending a license term is categorically excluded from review under the National Environmental Policy Act.

FERC addresses arguments raised on rehearing

C-7, *Rio Grande LNG, LLC*, Docket No. CP16-454-002. The order modifies and sustains the result of an August 13, 2020 Commission staff letter order accepting Rio Grande LNG's request to reduce the number of liquefaction trains from six to five trains at the Rio Grande LNG terminal in Cameron County, Texas.

FERC amends authorization for a liquefied natural gas project

C-12, *Golden Pass LNG Terminal LLC*, Docket No. CP20-459-000. The order amends Golden Pass LNG Terminal's Natural Gas Act section 3 authorization to increase the total liquefied natural gas production capacity of its three liquefaction trains from 15.6 million tonnes per annum (mtpa) to 18.1 mtpa. The increased capacity results from capturing design margins and more efficient maintenance processes and will not require any construction or modification of the facilities.

FERC denies petition for a declaratory order

C-15, *PennEast Pipeline Company, LLC*, Docket No. CP20-518-000. The order denies the petition of Robert Kaiser who requested the Commission issue an order declaring that PennEast be prohibited from exercising eminent domain authority until PennEast has received the necessary permits and authorizations to commence construction.

FERC denies petition for a declaratory order

C-16, *Pacific Connector Gas Pipeline, LP and Jordan Cove Energy Project L.P.*, Docket Nos. CP17-494-003 and CP17-495-003. In their petition, Jordan Cove and Pacific Connector request that the Commission find that the Oregon Department of Environmental Quality waived its authority to issue a Clean Water Act section 401 certification for the Jordan Cove Energy Project. The order finds that Jordan Cove and Pacific Connector never requested certification with respect to the Commission authorizations for the Jordan Cove Energy Project and that the Oregon Department of Environmental Quality could not have waived its authority to issue certification for a request it never received.

FERC dismisses a complaint

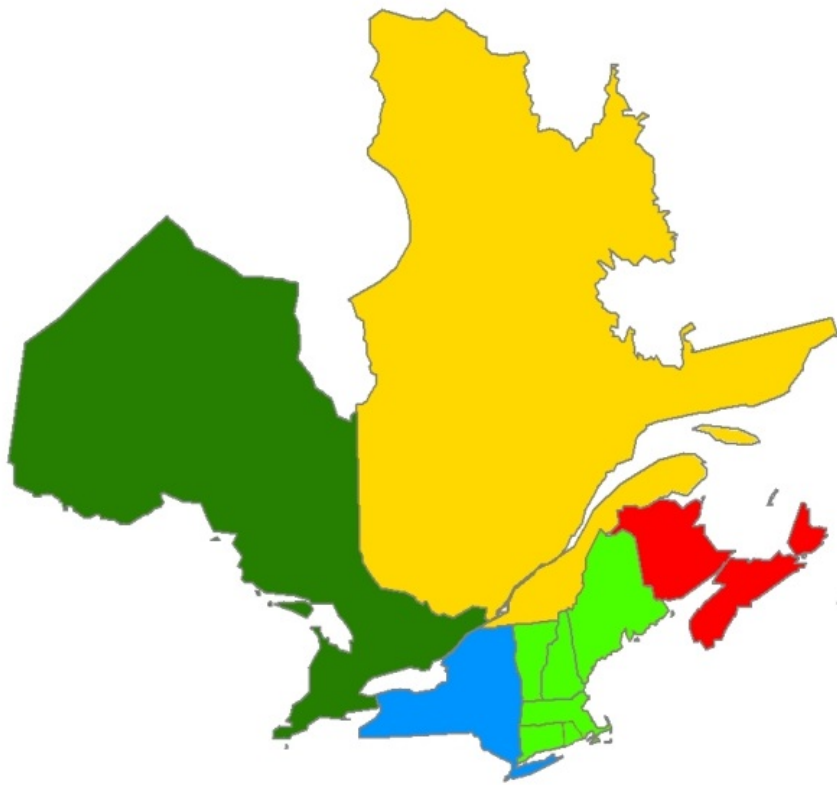
C-18, *Spire STL Pipeline LLC*, Docket No. CP17-40-005. The order denies a July 3, 2019 complaint filed by Central Land Consulting, LLC (Central Land) concerning the construction of the Spire STL Pipeline Project. Among other things, Central Land's complaint asserts that Spire STL Pipeline LLC and the Commission failed to consider landowners' prior allegations of environmental non-compliance as formal complaints under Rule 206 of the Commission's Rules of Practice and Procedure. The order dismisses Central Land's complaint, finding that it failed to establish standing and constituted an impermissible collateral attack on several delegated letter orders issued by the Chief of Gas Branch 4, Division of Gas — Environment and Engineering in FERC's Office of Energy Projects.



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)

2021 Business Plan and Budget



Draft #1
Submitted to NERC May 6, 2020

Table of Contents

Introduction.....	3
Personnel Analysis.....	14
Section A — 2021 Regional Entity Division Business Plan and Budget	17
Reliability Standards Program	17
Compliance Monitoring and Enforcement and Organization Registration and Certification Program.....	22
Reliability Assessment and Performance Analysis Program.....	28
Training, Education, and Operator Certification Program.....	36
Situation Awareness and Infrastructure Security Program	41
Administrative Services	49
Technical Committees and Member Forums	51
General and Administrative	52
Legal and Regulatory	53
Information Technology	54
Human Resources	56
Accounting and Finance	57
Regional Entity Assessment Analysis	58
Section B – Supplemental Financial Information.....	62
Reserve Balance.....	62
Breakdown by Statement of Activity Sections	63
Section C — Criteria Services Division Activities.....	70
Personnel Analysis.....	78
Reserve Analysis.....	79
Section D — Additional Financial Statements	81
Statement of Financial Position	81
Appendix A Staff Allocations.....	82
Appendix B Acronyms	84
Appendix C Index of Figures and Tables.....	86

Introduction

Total NPCC Resources (in whole dollars)				
	2021 Budget	U.S.	Canada	Mexico
Regional Entity Division FTEs	43.11			
Criteria Services Division FTEs	2.14			
Total FTEs	45.25			
Regional Entity Division Expenses	\$16,665,063			
Criteria Services Division Expenses	\$1,015,252			
Total Expenses	\$17,680,315			
Regional Entity Division Inc(Dec) in Fixed Assets	\$94,000			
Criteria Services Division Inc(Dec) in Fixed Assets	\$6,000			
Total Inc(Dec) in Fixed Assets	\$100,000			
Regional Entity Division Working Capital Requirement**	(\$574,418)			
Criteria Services Division Working Capital Requirement***	(\$311,055)			
Total Working Capital Requirement	(\$885,473)			
Total Regional Entity Division Funding Requirement	\$16,184,645			
Total Criteria Services Division Funding Requirement	\$710,197			
Total Funding Requirement	\$16,894,842			
Regional Entity Division Assessments	\$15,456,870	XXXX,XXX	XXXX,XXX	
Regional Entity Division Assessments Percentage	100%	XX.X%	XX.X%	
Criteria Services Division Membership Fees	\$706,472	XXXX,XXX	XXXX,XXX	
Total NPCC Assessments & Membership Fees	\$16,163,342	XXXX,XXX	XXXX,XXX	
NEL	XX	XX	XX	
NEL %	100%	XX.XX%	XX.XX%	

** Refer to Table B-1 on page 62 in Section B.

*** Refer to the Reserve Analysis on page 79 in Section C.

2021 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 no change to its total operating budget and a decrease in assessments of -1.5%. Additional 2021 succession implementation costs will be funded through existing Business Continuity Reserves, having no impact on assessments, and are excluded from the operating budget change calculation. On a divisional level, NPCC proposes a Regional Entity budget and assessment increase of 0.8% and a Criteria Services division budget decrease of -11.2% and assessment decrease of -33.7%. Criteria Services assessments are decreasing by a percentage greater than decrease in budget in order to reduce operating reserves in accordance with the established policy range. Additional detail regarding reserve balances for the Regional Entity and Criteria Services divisions can be found on pages 62 and 79, respectively. The proposed 2021 funding requirements will be satisfied by a Regional Entity division assessment of \$15,456,870 and Criteria Services division membership fees of \$706,472, for a total of \$16,163,342. The total NPCC assessments and fees represent a decrease of -1.5% compared to the 2020 total assessments and fees of \$16,403,939. 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 Northeastern North America 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 46% U.S. and 54% Canadian. With regard to Canada, approximately 70% of Canadian net energy for load is within the NPCC Region.

Effective January 1, 2016, NPCC executed an Amended and Restated Regional Delegation Agreement with the North American Electric Reliability Corporation (NERC or Electric Reliability Organization "ERO" 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 (MOU) or Agreements with Canadian provincial regulatory and/or governmental authorities in Ontario, Québec, New Brunswick and Nova Scotia.

An Amended and Restated Delegation Agreement effective as of January 1, 2021, between the North American Electric Reliability Corporation ("NERC") and NPCC is expected to be executed later in 2020 indicating that NPCC meets all requirements of Section 215 of the Federal Power Act, the ERO Regulations, and the NERC Rules of Procedure as approved by the Federal Energy Regulatory Commission necessary to qualify for delegation for the coming five year period. This amended and restated Agreement will incorporate the benefits of the NPCC and NERC mutual experience and lessons learned while operating under the predecessor agreement with regard to NPCC U.S. and thereby provide for the more efficient and effective execution of respective responsibilities in a transparent manner that is pursuant to Section 215 and ERO Regulations. It is imperative that NPCC maintain its ability to carry out delegated authorities and responsibilities. NPCC has a 2021 targeted staffing level of 45.25 power industry professionals and support personnel. Details of the 2021 business plans and budget for each program area are included in Section A for the Regional Entity division. The 2021 Regional Entity division supplemental financial schedules are shown in Section B. Section C details the 2021 Criteria Services division business plan and budget.

Membership and Governance

NPCC monitors approximately 243 registered entities and some 496 functions in the Region for compliance with mandatory Reliability Standards. NPCC currently has approximately 95 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.

Under the Criteria Services division, NPCC will seek out and evaluate for membership, entities involved in emerging technologies to assure that those entities that have an impact on Bulk Electric System reliability are included in appropriate NPCC activities.

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, pension, governance, compensation and human resource matters consistent with their approved charters. The Board endorses a non-employee, Certified Public Accountant for election by the NPCC Members as Treasurer of the corporation. An independent director chairs the FAC and works with the Chief Operating Officer who provides oversight of the finances of the corporation. The FAC Chair along with the CPA Treasurer and Chief Operating Officer report 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* establish 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 individual provincial MOU or Agreements with each province providing the unique parameters for compliance and enforcement activities for each of the provinces. An 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 implementation of the Québec reliability standards compliance monitoring and enforcement program. 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 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. 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 2009 Agreement). Under the terms of the 2009 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, NERC and NPCC are parties to the September 24, 2014 *Agreement on the Implementation of the Québec Reliability Standards Compliance Monitoring and Enforcement Program* (the 2014 Agreement). Through the 2014 Agreement, the Régie de l'énergie retains the services of NPCC to monitor and assess the compliance of registered entities in Québec with the reliability standards adopted by the Régie with respect to electric power transmission in Québec.

On April 1, 2015, the Québec Reliability Standards Compliance Monitoring and Enforcement Program ("QCMEP"), which was developed jointly by the Régie de l'énergie, NPCC and NERC, came into effect. Together, the 2014 Agreement and the QCMEP detail the procedures and

program for monitoring and enforcing mandatory electric power transmission reliability standards in Québec.

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 Contrôle des mouvements d'énergie (HQCME), a division of Hydro-Québec TransÉnergie, as the Reliability Coordinator for Québec. In accordance with its mandate and as recognized in the 2009 Agreement, it is this entity that is responsible for the filing with the Régie de l'énergie for approval of reliability standards in Québec. HQCME has filed for the approval of certain reliability standards and the Régie de l'énergie has made certain reliability standards mandatory in Québec and is continuing proceedings to make additional reliability standards mandatory in Québec.

NPCC also conducts 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

On 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 New Brunswick Energy and Utilities Board (NBEUB) is an independent, quasi-judicial board that is responsible for regulating New Brunswick’s electricity sector under the NB Electricity Act. The NBEUB has the responsibility to adopt and enforce reliability standards in New Brunswick.

As contemplated in the NB Electricity Act, NPCC and the NBEUB entered into a Service Contract dated August 10, 2016, whereby NPCC provides CMEP and other services for the NBEUB. Additionally, the NBEUB, NPCC, and NERC entered into a Memorandum of Understanding on August 10, 2016, which describes the roles and responsibilities of the three entities and facilitates data sharing. These two documents, along with the NB Electricity Act are the governing documents with respect to conducting CMEP and other reliability related activities in New Brunswick.

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 NB Power 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 FERC. The NBEUB 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 NBEUB considers relevant. The Electricity Act requires the NBEUB to notify NPCC and NERC of an application by NB Power 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 provides for NPCC to identify entities that must register with the NBEUB in the New Brunswick specific registry. Additionally, NPCC may carry out the compliance monitoring and assessment for the NBEUB and assist and advise the enforcement for the NBEUB, including financial penalties. NPCC is also permitted to carry out or exercise any power in the implementing regulations that is specific to the NBEUB, as provided for in the Service Contract. 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 and enforcement activities with respect to the standards and forward any non-compliance information and recommendations to the NSUARB. The NSUARB maintains the final authority with respect to enforcement in Nova Scotia and based on the recommendations from NPCC, may determine whether a violation has occurred and, if so, what remedial measures or non-monetary penalties should be imposed.

ERO Enterprise Model and Transformation

The collective network of leadership, experience, skills, and technologies shared among NERC and the Regional Entities is referred to as the ERO Enterprise. The ERO Enterprise is a collaborative organization with distinct roles between NERC and the Regional Entities. The ERO Enterprise strives for consistency where necessary, but recognizes that each Regional Entity addresses reliability in unique ways based on its own challenges and stakeholder needs; the model enables innovative and distinctive approaches to address these unique reliability risks and challenges locally. As the ERO Enterprise continues to mature, the organization is working on a transformation initiative to further leverage resources, enhance communication and collaboration, and ensure grid reliability. A set of declarations was established in 2019, committing the ERO Enterprise to:

- Work together as one team and honor each of its roles;
- Actively support ERO Enterprise activities while eliminating unnecessary duplication of work;
- Collaborate to develop clear and consistent guidance across the ERO Enterprise;
- Share information, knowledge, and resources across the ERO Enterprise;
- Develop and share harmonized messages across ERO Enterprise communications; and
- Support innovation, initiatives, and the sharing of best-practices across the ERO Enterprise.



NERC has unique responsibilities to oversee program areas, set qualifications and expectations for the performance of delegated activities, and assess, train, and give feedback to corresponding Regional Entity programs. NERC and the Regional Entities also coordinate activities to identify, prioritize, and address risks to reliability. The Regional Entities have a mirrored set of responsibilities within the ERO Enterprise model, providing input into the overall development of each ERO program area, providing training and development to meet ERO qualifications, and ensuring delegated responsibilities are completed. Regional Entities also have an obligation to meet professional standards of independence and objectivity and provide the best available expertise for addressing regional risks.

ERO Enterprise Long-Term Strategy

NERC and the Regional Entities are continually refining their individual and collective operating and governance practices in support of strategic and operational goals and objectives that are designed to ensure the ERO fulfills its statutory obligations. This collaboration is done while acknowledging the unique differences across the Regions, and the different corporate and governance responsibilities of each entity.

In 2019, ERO Enterprise leadership came together to revise the *ERO Enterprise Long-Term Strategy* as part of an effort to streamline its strategic and operational documents and ensure alignment with the NERC Reliability Issues Steering Committee's (RISC's) currently identified bulk power system (BPS) risks. This strategy, which was approved by the NERC Board of Trustees on December 12, 2019, can be found within the NERC Business Plan and Budget, and includes the following strategic focus areas:

1. Expand risk-based focus in all standards, compliance monitoring, and enforcement programs;
2. Assess and catalyze steps to mitigate known and emerging risks to reliability and security, leveraging the RISC's biennial *ERO Reliability Risk Priorities Report*;
3. Build a strong, Electricity Information Sharing and Analysis Center (E-ISAC)-based security capability;
4. Strengthen engagement across the reliability and security ecosystem in North America; and
5. Capture effectiveness, efficiency, and continuous improvement opportunities.

As part of the business planning and budgeting process, NERC and the Regional Entities identify and discuss departmental goals and activities to ensure alignment with the long-term strategy and harmonization across the ERO Enterprise where appropriate. Program area narratives in each

organization's business plan and budget may reference how activities support each of the strategic focus areas.

2021 Key Goals and Key Deliverables

NPCC activities that support ERO Enterprise Long-Term Goals are detailed in each of the following program area sections. For example, key goals and deliverables within the Reliability Standards program area include supporting the development of risk-responsive Reliability Standards as well as facilitating a Distributed Energy Resources (DER) Forum. Within the Compliance Monitoring and Enforcement and Organization Registration and Certification program, in addition to conducting objective, risk-informed compliance monitoring, enforcement and entity registration activities, this area will be addressing increased reliability enhancement activities and implementing the ERO Enterprise CMEP data application (Align). The Reliability Assessment and Performance Analysis program will be focusing on reduction of known risks to reliability and the identification and assessment of emerging reliability risks, such as changing resource composition. In the Situation Awareness and Infrastructure Security area there is an increasing focus on the identification and reduction of cyber and physical security risks through expanded outreach. In an order to achieve these goals and expanded efforts, while minimizing increases in budget, significant reprioritization within the business plan and reallocation of resources were required.

Regional Entity Division Functional Scope

NPCC's Regional Entity division functions in support of the ERO include:

- Active participation in the development and revision of North American Reliability Standards for the bulk electric system, and as needed development of Reliability Standards and Variances 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 bulk electric infrastructure.
- Participating in reliability and security activities that enhance resilience of the bulk power system.

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, in conjunction with NERC and the other Regional Entities, has developed and deployed an ERO Enterprise-wide CMEP data application (Align) for gathering data, analysis, and tracking of compliance information to carry out these responsibilities in a consistent and cost-effective manner.

NPCC has organized the remaining staff into program areas consistent with EPAAct 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.

2021 Overview of Regional Entity Division Cost Impacts

The proposed Regional Entity division assessment of \$15,456,870, to support the Regional Entity division operating budget of \$16,281,543, is an increase of 0.8% compared to the 2020 assessment of \$15,338,737.

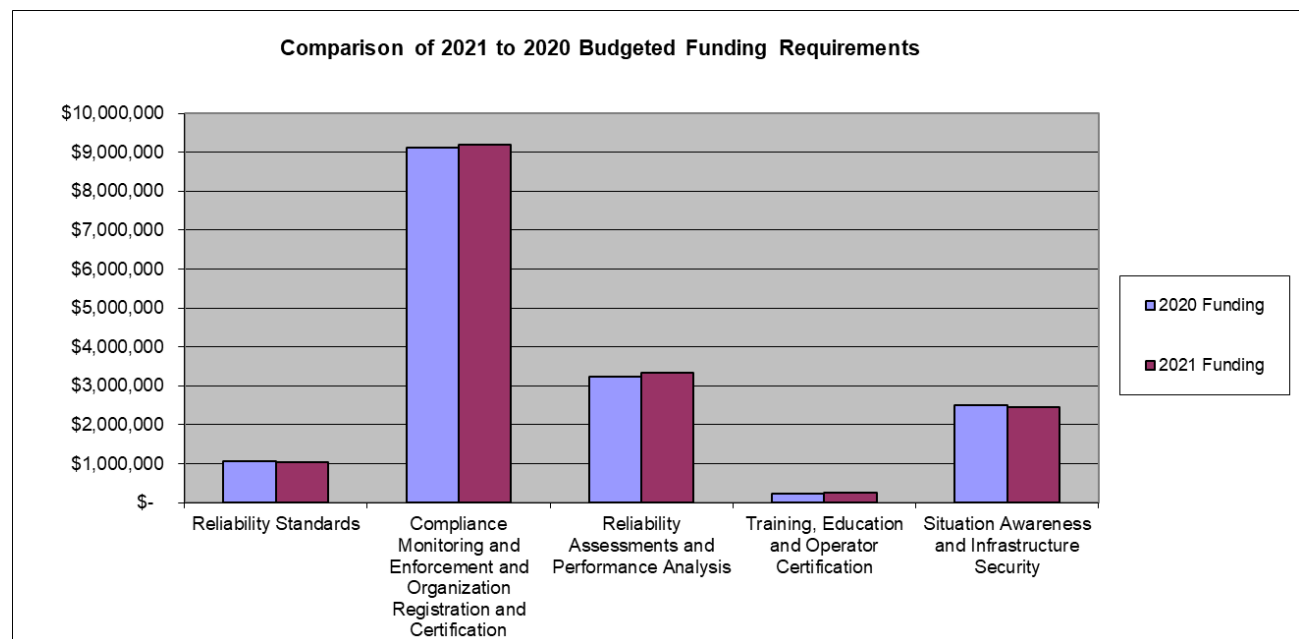
2020 Projections

Current year projections are taken into consideration in development of the budget. Expenses are currently projected to be on budget in all areas or slightly under budget. 2020 Projections reflect expectations based on the first quarter variance report. It is anticipated that projections could change throughout 2020 and would be reflected in each subsequent quarter's variance report. The full health and subsequent financial impacts of the COVID-19 pandemic to the NPCC Region are currently unknown.

Summary by Program

Program	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Reliability Standards	\$ 1,071,015	\$ 1,071,015	\$ 1,038,118	\$ (32,897)	-3.1%
Compliance Monitoring and Enforcement and Organization Registration and Certification	\$ 9,109,633	\$ 8,922,633	\$ 9,190,590	\$ 80,956	0.9%
Reliability Assessments and Performance Analysis	\$ 3,231,169	\$ 3,231,169	\$ 3,342,004	\$ 110,835	3.4%
Training, Education and Operator Certification	\$ 239,412	\$ 239,412	\$ 248,621	\$ 9,209	3.8%
Situation Awareness and Infrastructure Security	\$ 2,505,877	\$ 2,443,877	\$ 2,462,210	\$ (43,668)	-1.7%
Total	\$ 16,157,107	\$ 15,908,107	\$ 16,281,543	\$ 124,436	0.8%

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

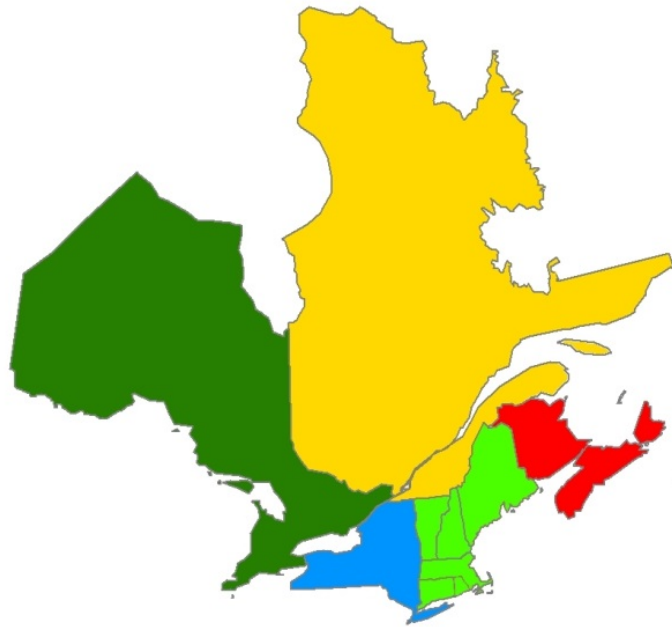
Total FTE's by Program Area	Budget 2020	Projection 2020	Direct FTEs 2021 Budget	Shared FTEs ¹ 2021 Budget	Total FTEs 2021 Budget	Change from 2020 Budget
REGIONAL ENTITY DIVISION						
Operational Programs						
Reliability Standards	1.93	1.93	1.00	0.94	1.94	0.01
Compliance Monitoring and Enforcement and Organization Registration and Certification	18.00	17.45	19.45	0.00	19.45	1.45
Training, Education, and Operator Certification	0.10	0.10	0.10	0.00	0.10	0.00
Reliability Assessment and Performance Analysis	5.43	5.43	4.50	0.94	5.44	0.01
Situation Awareness and Infrastructure Security	5.40	5.40	5.40	0.00	5.40	0.00
Total FTEs Operational Programs	30.86	30.31	30.45	1.88	32.33	1.47
Administrative Programs						
Technical Committees and Member Forums	0.50	0.50	0.50	0.00	0.50	0.00
General and Administrative	2.73	3.23	3.00	0.23	3.23	0.50
Information Technology	2.00	2.55	2.55	0.00	2.55	0.55
Legal and Regulatory	2.00	2.00	2.00	0.00	2.00	0.00
Human Resources	1.00	0.50	0.50	0.00	0.50	-0.50
Accounting and Finance	2.00	2.00	2.00	0.00	2.00	0.00
Total FTEs Administrative Programs	10.23	10.78	10.55	0.23	10.78	0.55
Total FTEs	41.09	41.09	41.00	2.11	43.11	2.02

¹A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

2020 Budget and Projection and 2021 Budget Comparisons

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
REGIONAL ENTITY DIVISION						
	2020 Budget	2020 Projection	Variance ⁽²⁾ 2020 Projection v 2020 Budget Over(Under)	2021 Budget ⁽³⁾	Variance 2021 Budget v 2020 Budget Over(Under)	
Funding						
ERO Funding						
ERO Assessments	\$ 15,338,737	\$ 15,338,737	\$ -	\$ 15,456,870	\$ 118,133	
Penalty Sanctions ⁽¹⁾	120,000	120,000	-	604,000	484,000	
Total ERO Funding	\$ 15,458,737	\$ 15,458,737	\$ -	\$ 16,060,870	\$ 602,133	
Membership Dues	-	-	-	-	-	
Testing Fees	-	-	-	-	-	
Services & Software	-	-	-	-	-	
Workshops & Misc Revenue	67,500	33,750	(33,750)	67,500	-	
Interest & Investment Income	55,800	55,800	-	56,275	475	
Total Funding (A)	\$ 15,582,037	\$ 15,548,287	\$ (33,750)	\$ 16,184,645	\$ 602,609	
Expenses						
Personnel Expenses						
Salaries	\$ 7,704,262	\$ 7,544,262	\$ (160,000)	\$ 8,073,535	\$ 369,273	
Payroll Taxes	479,019	462,019	(17,000)	493,288	14,269	
Benefits	1,943,385	1,895,385	(48,000)	2,035,447	92,063	
Retirement Costs	882,950	858,950	(24,000)	920,033	37,083	
Total Personnel Expenses	\$ 11,009,617	\$ 10,760,617	\$ (249,000)	\$ 11,522,303	\$ 512,687	
Meeting Expenses						
Meetings & Conference Calls	\$ 397,750	\$ 332,750	\$ (65,000)	\$ 381,000	\$ (16,750)	
Travel	845,900	845,900	-	884,200	38,300	
Total Meeting Expenses	\$ 1,243,650	\$ 1,178,650	\$ (65,000)	\$ 1,265,200	\$ 21,550	
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ 2,071,150	\$ 2,071,150	\$ -	\$ 1,509,800	\$ (561,350)	
Office Rent	832,700	832,700	-	870,141	37,441	
Office Costs	685,981	685,981	-	837,420	151,439	
Professional Services	947,000	947,000	-	1,005,000	58,000	
Computer & Equipment Leases	-	-	-	-	-	
Miscellaneous	51,000	51,000	-	51,000	-	
Total Operating Expenses, excluding Depreciation	\$ 4,587,831	\$ 4,587,831	\$ -	\$ 4,273,361	\$ (314,470)	
Total Direct Expenses	\$ 16,841,098	\$ 16,527,098	\$ (314,000)	\$ 17,060,864	\$ 219,767	
Indirect Expenses	\$ (409,450)	\$ (409,450)	\$ -	\$ (395,801)	\$ 13,649	
Other Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	\$ -	
Total Expenses (B)	\$ 16,431,647	\$ 16,117,647	\$ (314,000)	\$ 16,665,063	\$ 233,416	
Change in Net Assets (=A-B)	\$ (849,611)	\$ (569,361)	\$ 280,250	\$ (480,418)	\$ 369,193	
Fixed Asset Additions, excluding Right of Use Assets (C)	\$ 170,000	\$ 170,000	\$ -	\$ 94,000	\$ (76,000)	
TOTAL BUDGET (=B+C)	\$ 16,601,647	\$ 16,287,647	\$ (314,000)	\$ 16,759,063	\$ 157,416	
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ (1,019,611)	\$ (739,361)	\$ 280,250	\$ (574,418)	\$ 445,193	
⁽¹⁾ \$604,000 of penalty sanctions collected to date and prior to June 30, 2020.						
⁽²⁾ 2020 Projections reflect expectations based on the first quarter statement of activities. It is anticipated that projections could change throughout 2020 and would be reflected in each subsequent quarter's statement of activities.						
⁽³⁾ 2021 Budget includes non-recurring succession planning costs in the amount of \$477,520 to be funded from existing Business Continuity Reserves, having no impact on assessments. The 2021 total operating budget exclusive of non-recurring succession planning costs is \$16,281,543.						

Section A – Regional Entity Division 2021 Business Plan and Budget



Section A — 2021 Regional Entity Division Business Plan and Budget

Reliability Standards Program

Reliability Standards Program Resources			
(in whole dollars)			
	2020 Budget	2021 Budget	Increase (Decrease)
Total FTEs	1.93	1.94	0.01
Direct Expenses	\$693,683	\$673,667	(\$20,015)
Indirect Expenses	\$366,700	\$358,810	(\$7,890)
Other Non-Operating Expenses	\$0	\$0	\$0
Fixed Asset Additions	\$10,632	\$5,641	(\$4,991)
Total Funding Requirement	\$1,071,015	\$1,038,118	(\$32,897)

Program Scope and Functional Description

The NPCC Reliability Standards Program Area operates in accordance with NPCC’s filed and approved Regional Delegation Agreement and NERC Rules of Procedure Section 300. The program supports the ERO Standards Program Area roles and responsibilities, the ERO Enterprise Long-Term Strategy and aligns with NPCC’s Strategic Plan and Board of Director goals. NPCC’s Reliability Standards Program Area provides an efficient and effective mechanism for stakeholders to provide input and facilitate the development of, and improvement to, NERC and Regional reliability standards. NPCC works with the ERO and its stakeholders to expand the risk-based focus in all standards. The primary objectives of NPCC’s Reliability Standards Program Area are to support the development of ERO standards and Regional variances which establish “results-based” requirements and continue to deliver a high level of BPS reliability and security, with no identified gaps, and with due consideration given to cost effectiveness. NPCC supports the ERO efforts to develop reliability standards in a timely and efficient manner and which are also responsive to FERC Directives and industry risk.

At the Regional level, the standards program area develops, and maintains NPCC Regional Reliability Standards, and ERO Standards Variances for the northeast as required. The NPCC Reliability Standards Program Area also provides oversight to ensure that NPCC’s Regional Reliability Criteria contained in the form of Directories, are developed, approved, and maintained as necessary to implement, augment, or to facilitate compliance with NERC Reliability Standards. NPCC’s reliability criteria are not reliability standards but are mandatory and subject to enforcement as outlined in the NPCC *Amended and Restated Bylaws* and various ISO tariffs, and individual interconnection agreements, as well as other executed contractual agreements. Regional Reliability Criteria may also address issues not within NERC’s statutory jurisdiction for Reliability Standards, such as resource adequacy, and conform to requirements in Section 313 of the NERC Rules of Procedure.

In addition, the NPCC Reliability Standards Program Area has been conducting Distributed Energy Resources (DER) Forums. Conventional fossil fuel units and nuclear retirements are increasingly being replaced by Variable Energy Resources on the transmission system and DER on the distribution system. DER is commonly referred to as “grid edge resources” and has introduced the concept of decentralized generation. It is projected that the future reliable operation of the BES, as defined in the US Federal Power Act, will be increasingly dependent on these

resources. The control systems of DER introduce new capabilities that could enhance reliability and understanding interoperability issues between transmission and distribution systems will become increasingly important. NPCC is engaged in a number of areas to promote their reliable integration into the BES and opportunities to provide industry guidance for interconnecting DER.

2021 Key Assumptions

- The number of continent-wide Reliability Standards development projects is expected to remain relatively stable, except as required to address any new FERC directives to create or modify Reliability Standards, or industry submittals of standard authorization requests. Also, there will be continued development activity on Cyber standards and it is expected some new standards will be developed related to cold weather preparedness and resilience (hardening for Electromagnetic Pulse – EMP, and other high impact low frequency events).
- Continent-wide Reliability Standards projects will consist primarily of acting on recommendations of the various phases of the Standards Efficiency Review project, Standards Grading activities, conducting periodic reviews on existing Reliability Standards to improve their content and quality, responding to identified risks to reliability (including those that may be identified through the implementation of risk-based Compliance Monitoring and Enforcement), and addressing FERC directives that may arise.
- NPCC’s Regional Reliability Standards development activity is expected to remain at a stable level, driven by requests that the Regional Entity may receive or reliability issues that are identified and not under consideration by NERC. Creation of Variances to NERC Reliability Standards to address reliability concerns or to recognize the unique topology and reliability considerations of the Northeast (i.e. Québec’s recognition as an asynchronous interconnection within NPCC’s footprint) will be performed as necessary.
- The number of NERC and Regional standards interpretations is expected to remain low. Compliance Implementation Guidance documents, which provide approaches to being compliant with NERC Reliability Standards may be developed using NPCC’s open process and other industry vetting practices. These guidance documents are currently being developed by industry and the Standard Drafting Teams, and the number of requests may increase. The NPCC Reliability Standards program area will assist and facilitate support of these activities.
- Consistent with the NERC Rules of Procedure Sections 312 and 313, as continent-wide standards continue to evolve, NPCC Regional Standards and Criteria will need to be continually reviewed to ensure they augment but do not add redundancy to the ERO standards.

2021 Goals and Key Deliverables

- Participate in the annual development and revision of the NERC’s three-year Reliability Standards Development Plan (RSDP) through review, commenting, and other RSC activities.
- Participate in the NERC Standards Committee, as a representative for NPCC Regional stakeholders to advance strategic initiatives, to measure the effectiveness and quality of standards, support ERO efforts to address outstanding FERC Directives, and provide input in the prioritization of standards development projects.
- Support further development of cost effectiveness principles processes and pilots. Continue to provide insights to NERC, based on NPCC experiences, regarding strategy for developing cost effectiveness analysis for standards and identify opportunities to identify cost of risk mitigation for the draft standards.

-
- Participate in the NERC Standards Efficiency Review Project to retire standard requirements that are duplicative, administrative and add no additional benefit to the reliable operation of the bulk electric system.
 - Participate in the development of ERO Reliability Standards specified in NERC’s three-year Reliability Standards Development 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 under development or revision by leveraging existing NPCC Task Forces and subject matter experts and coordinate NPCC comments for Northeastern North America.
 - Participate in the Periodic Review Standing Team’s grading efforts and coordinate and represent the Regional and interregional input.
 - Assist NERC’s review of all industry “Requests for Interpretations” of NERC Reliability Standards.
 - NPCC staff and Regional drafting team volunteers will participate in the drafting of all ERO standards and provide support for development of improvements to standards. Those chosen to participate in drafting of standards will provide a point of contact for the NPCC Regional input to the standard being developed.
 - NPCC and its members will review and coordinate comments on FERC staff informal assessments of the ERO Enterprise as appropriate.
 - Participate in pre-ballot reviews of ERO standards and coordinate the development of consensus recommendations of the NPCC Members to the NERC Standards Drafting Team (SDT) and provide a list of any unaddressed issues to allow the Members to cast a ballot based on regional concerns to enhance the efficiency of the ERO standards development projects.
 - Review and identify issues and concerns raised in FERC NOPRs and NOIs for any and all standards related issues as appropriate.
 - 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 such as the North American Generator Forum and North American Transmission Forum when requested.
 - Monitor the NERC Reliability Issues Steering Committee (RISC) activities as they identify emerging risks and develop recommended actions to mitigate such risks. Provide a Regional point of contact for all potential reliability related risks and gaps within the Northeast or as noted by NPCC’s stakeholders.
 - Participate in and provide support to critical standards projects, such as CIP Supply Chain, Facility Ratings (IROL and SOL development), Geomagnetic Disturbances, High Altitude Electromagnetic Pulse (HEMP), changes to standards driven by inverter based DERs, etc.
 - Identify opportunities and initiate Regional Variances to the NERC Reliability Standards as soon as possible, allowing incorporation into the continent-wide standard during the development process.
 - Conduct reviews of Regional Standards as necessitated by the revision and approval of any associated Continent-wide NERC reliability standards or further reliability related need.
 - Conduct the development of any Québec Interconnection-Wide variances to NERC continent-wide standards using the NPCC Reliability Standards Development Process.
 - Identify potential reliability benefits and impacts to the BES as a result of DER penetration.
 - Conduct ongoing DER Forum activities to solicit and identify both opportunities and challenges to enhancing reliability through education, promotion of awareness and developing guidance, particularly for interconnection of utility scale DER on the Distribution System.
-

- Update, maintain and revise the NPCC DER guidance document as necessary and promote consistency across the NPCC footprint where possible.
- In conjunction with the Reliability Coordinating Committee, review any DER impacts identified by stakeholders and develop an approach to promote awareness and resolution of any issues.
- Identify opportunities to improve resilience of the BES and develop potential approaches either with the ERO or within the Region.
- Monitor state and provincial proceedings as they relate to the deployment of DER to meet emissions targets (e.g. New York Dept. of Public Service Interconnection Technical Working Work, Massachusetts Technical Standards Group, etc.)
- Identify and coordinate reliability related issues with applicable governmental authorities.
- Ensure the topics addressed by the Reliability Standards align with changing industry and reliability objectives.
- Participate in reliability metrics developmental activities to identify potential measures for benchmarking of reliability and standards to determine if an adequate level of reliability is being achieved through the Enhanced Periodic Review Standing Review Team activities.
- Identify opportunities and processes for cost-effectiveness analysis activities to determine the need to revise a standard during the Periodic Review or Standards Grading efforts.
- Identify any emerging interconnection-wide reliability issues which may need standards solutions and forward to the NERC Reliability Issues Steering Committee for their consideration.
- Identify opportunities to increase reliability or mitigate emerging risk through the revision of standards and their associated requirements.
- Identify any North American Electric Standards Review Board (NAESB) activities which may impact ERO standards.
- Identify potential market related issues that reliability standards or DER may cause during the NPCC RSC coordination and review process.
- Participate in NPCC Compliance and Standards Workshops and any NERC workshops and webinars to promote industry awareness.

Based on the portion of professional/technical staff time and other resources devoted to Reliability Standards development, NPCC estimates that it will expend approximately 6% of its resources on this activity.

Resource Requirements

- No significant changes.

Reliability Standards Program

Funding sources and related expenses for the Reliability Standards section of the 2021 business plan are shown in the table below. Explanations of variances by expense category are included with the Supplemental Tables found in Section B.

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
Reliability Standards						
	2020 Budget	2020 Projection	Variance 2020 Projection v 2020 Budget Over(Under)	2021 Budget	Variance 2021 Budget v 2020 Budget Over(Under)	
Funding						
ERO Funding						
ERO Assessments	\$ 1,063,510	\$ 1,063,510	\$ -	\$ 1,001,874	\$ (61,636)	
Penalty Sanctions	7,505	7,505	-	36,244	28,739	
Total ERO Funding	\$ 1,071,015	\$ 1,071,015	\$ -	\$ 1,038,118	\$ (32,897)	
Membership Dues	-	-	-	-	-	
Testing Fees	-	-	-	-	-	
Services & Software	-	-	-	-	-	
Workshops & Misc Revenue	-	-	-	-	-	
Interest & Investment Income	-	-	-	-	-	
Total Funding (A)	\$ 1,071,015	\$ 1,071,015	\$ -	\$ 1,038,118	\$ (32,897)	
Expenses						
Personnel Expenses						
Salaries	\$ 400,744	\$ 400,744	\$ -	\$ 389,334	\$ (11,410)	
Payroll Taxes	23,034	23,034	-	22,789	(244)	
Benefits	110,172	110,172	-	118,092	7,919	
Retirement Costs	43,833	43,833	-	41,453	(2,380)	
Total Personnel Expenses	\$ 577,783	\$ 577,783	\$ -	\$ 571,667	\$ (6,115)	
Meeting Expenses						
Meetings & Conference Calls	\$ 5,000	\$ 5,000	\$ -	\$ 5,000	\$ -	
Travel	90,900	90,900	-	75,000	(15,900)	
Total Meeting Expenses	\$ 95,900	\$ 95,900	\$ -	\$ 80,000	\$ (15,900)	
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ 20,000	\$ 20,000	\$ -	\$ 20,000	\$ -	
Office Rent	-	-	-	-	-	
Office Costs	-	-	-	2,000	2,000	
Professional Services	-	-	-	-	-	
Computer & Equipment Leases	-	-	-	-	-	
Miscellaneous	-	-	-	-	-	
Total Operating Expenses, excluding Depreciation	\$ 20,000	\$ 20,000	\$ -	\$ 22,000	\$ 2,000	
Total Direct Expenses	\$ 693,683	\$ 693,683	\$ -	\$ 673,667	\$ (20,015)	
Indirect Expenses	\$ 366,700	\$ 366,700	\$ -	\$ 358,810	\$ (7,890)	
Other Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	\$ -	
Total Expenses (B)	\$ 1,060,383	\$ 1,060,383	\$ -	\$ 1,032,478	\$ (27,905)	
Change in Net Assets (=A-B)	\$ 10,632	\$ 10,632	\$ -	\$ 5,641	\$ (4,991)	
Fixed Asset Additions, excluding Right of Use Assets (C)	10,632	10,632	-	5,641	(4,991)	
TOTAL BUDGET (=B+C)	\$ 1,071,015	\$ 1,071,015	\$ -	\$ 1,038,118	\$ (32,897)	
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ 0	\$ 0	\$ -	\$ (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)			
	2020 Budget	2021 Budget	Increase (Decrease)
Total FTEs	18.00	19.45	1.45
Direct Expenses	\$5,590,473	\$5,536,689	(\$53,784)
Indirect Expenses	\$3,420,003	\$3,597,350	\$177,347
Other Non-Operating Expenses	\$0	\$0	\$0
Fixed Asset Additions	\$99,157	\$56,551	(\$42,606)
Total Funding Requirement	\$9,109,633	\$9,190,590	\$80,956

Program Scope and Functional Description

The NPCC Compliance Monitoring and Enforcement and Organization Registration and Certification Program (CORC) Program Area operates in accordance with NPCC's filed and approved Regional Delegation Agreement, the NERC Rules of Procedure, and individual Canadian Provincial MOUs and/or Agreements. The program supports Compliance Enforcement (Section 400) and Organization Registration and Certification (Section 500), the ERO Enterprise Long-Term Strategy, and aligns with NPCC Board of Director goals and strategies.

The CORC Program Area 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 risk-based NERC Compliance Monitoring and Enforcement Program (CMEP) data application (Align) in the United States, including the compliance monitoring, mitigation assessment and enforcement of NERC Reliability Standards and Regional Reliability Standards;
- 3) In accordance with the relevant memorandums of understanding (MOU's), the implementation of the risk-based NERC CMEP in Ontario and Nova Scotia, including the assessment and enforcement of NERC Reliability Standards and Regional Reliability Standards effective in those jurisdictions;
- 4) The implementation of the Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP), including the compliance monitoring, assessment and enforcement of NERC Reliability Standards and Regional Reliability Standards effective in Quebec; and
- 5) The implementation of the New Brunswick Compliance Monitoring and Enforcement Program (NBCMEP) in New Brunswick, including the compliance monitoring, assessment and enforcement recommendations of the NERC Reliability Standards and Regional Reliability Standards effective in New Brunswick.

Through the CORC Program Area, NPCC strives to be a strong enforcement authority that is independent, objective, fair, and promotes a culture of reliability excellence through risk-informed compliance monitoring, mitigation, enforcement, and registration. To accomplish this goal, CORC is divided into three sub-program areas: Compliance Fundamentals; Compliance Audits and Investigations; and Compliance Mitigation and Enforcement.

Compliance Fundamentals

The Compliance Fundamentals sub-program area is responsible for registration and certification activities and for general compliance activities that span across the other two sub-program areas. The Compliance Fundamentals sub-program area:

- Collaborate across the ERO through participation in the Risk Performance and Monitoring Group (RPMG), Enforcement Group (EG), Organization Registration and Certification Group (ORCG), and the development of the annual ERO CMEP staff workshop.
- Identifies and registers the BES owners, operators, and users that are required to comply with the NERC and Regional Reliability Standards,
- Conducts Certifications in accordance with the NERC ROP,
- Leads the development of the annual implementation plans (ERO Enterprise, Quebec, New Brunswick),
- Implements the ERO Enterprise registration tool (CORES -Centralized Organization Registration ERO System) and the ERO Enterprise CMEP data application (Align),
- Responds to any complaints submitted to NPCC,
- Maintains any NPCC specific compliance tools or programs needed,
- Conducts two stakeholder compliance workshops on an annual basis,
- Assesses compliance trends and conducts additional outreach, training, and education to support the implementation of Reliability Standards,
- Conducts Inherent Risk Assessments (IRA) on registered entities,
- Conducts formal Evaluations of Internal Controls (EIC) on volunteering registered entities,
- Develops Compliance Oversight Plans (COP) for registered entities,
- Assists with the development of the annual CMEP implementation plans,
- Provides the basis for each registered entity's Compliance Oversight Plan.

Compliance Audits and Investigations

The Compliance Audits and Investigations sub-program area is responsible for conducting all compliance monitoring activities. The Compliance Audits and Investigations sub-program area is focused on the most significant risks to the BPS. The Compliance Audits and Investigations sub-program area:

- Conducts NPCC compliance monitoring activities, including audits, spot checks, and guided self-certifications,
- Incorporates the results of the IRA and EIC into its compliance monitoring process,
- Assesses the maturity of the entity's internal controls during audits,
- Engages the entity on the maturity of the Internal Compliance Program
- Issues reports, including audit reports, spot check reports, guided self-certification reports,
- Implements and maintains the Critical Infrastructure Protection (CIP) Standards Technical Feasibility Exceptions process.

Compliance Mitigation and Enforcement

The Compliance Mitigation and Enforcement sub-program area is responsible for undertaking enforcement activities in accordance with risk-based approaches and conducting technical assessments of registered entities' plans and activities to mitigate noncompliance. Depending on the jurisdiction, enforcement either makes official recommendations to the appropriate regulatory authority or assists and coordinates with NERC to make such official recommendations. The Compliance Mitigation and Enforcement sub-program area:

- Determines the relevant facts and circumstances necessary to understand each noncompliance,

- Evaluates and assigns a risk level to each noncompliance,
- Advises on the level of mitigation required to prevent recurrence of the issue,
- Evaluates and approves the mitigation activities or Mitigation Plan(s) for each noncompliance,
- Assesses the relevant compliance history for each noncompliance,
- Determines the disposition method for each noncompliance,
- Conducts settlement negotiations,
- Calculates penalty sanctions in consistent fashion, and
- Evaluates registered entities for the self-logging program.

2021 Key Assumptions and Cost Impacts

2020	Projected 2021
8 On-Site O&P Audits	8 On-Site O&P Audits
10 On-Site CIP Audits	8 On-Site CIP Audits
40 Off-Site Audits	30 Off-Site O&P Audits
25 Off-Site CIP Audits	10 Off-Site CIP Audits
10 Spot Checks	13 Spot Checks
40 Self-certifications	60 Self-certifications
50 Inherent Risk Assessments	46 Inherent Risk Assessments
7 On-site O&P Internal Control Evaluations	8 Evaluations of Internal Controls
10 On-site CIP Internal Control Evaluations	50 Internal Compliance Program Reviews
225 Violations (Estimated)	225 Violations (Estimated)
Settlements Covering 80 Violations	Settlements Covering 80 Violations
	48 Compliance Oversight Plans (Full Implementation in 2021)
1 Hearings (Unbudgeted)	1 Hearings (Unbudgeted)
1 CI (Estimated)	1 CI (Estimated)
2 Entity Certifications	2 Entity Certifications

- Compliance Monitoring activities will be cost effectively addressed with the addition of two employee auditors (net increase of 1.45 compliance FTEs after the partial re-allocation of a compliance position to IT in 2020), offset by a decrease in independent contractor audit costs.
- The 2021 Business Plan projects the same level of enforcement processing activities as the 2020 Budget. It is expected that the increase in violation processing will also continue in 2021. This is partly due to the increase in the number of cyber systems that are in scope for compliance in most jurisdictions.
- One Compliance Investigation is projected for 2021. Compliance Investigations are manpower intensive for NPCC staff (requiring allocation of more resources and potentially higher than normal costs).

2021 Goals and Key Deliverables

- Conduct scheduled compliance monitoring and enforcement activities pursuant to the 2021 Implementation Plans.
- Continue applying risk-based approaches for CMEP, registration, and certification activities.

-
- Identify potential issues related to NERC Reliability Standards as a result of compliance monitoring, enforcement and event analysis activities.
 - Continue to implement compliance responsibilities in Canada based on the unique regulatory structure specific to each provincial and/or governmental jurisdiction.
 - Evaluate monitoring, violation processing, risk-assessment, registration and certification program for sufficiency and effectiveness. Modify as needed.
 - Collaborate within the ERO Enterprise to develop and implement a common and consistent CMEP data application (Align) for compliance processes, information systems, and methods among Regions.
 - Provide education and outreach to the registered entities on all CMEP, registration, and certification topics, including the development and implementation of the ERO Enterprise Registration tool (CORES – Centralized Organization Registration ERO System) and the Align CMEP data application.
 - Conduct two in-person Compliance Workshops.
 - Develop annual reports for QCMEP/CMEP activity in Québec and New Brunswick.
 - Develop and/or provide input on 2021 CMEP Implementation Plans (ERO Enterprise, Québec, New Brunswick).
 - Attend training necessary and/or beneficial to performing Registration, Certification, Entity Risk Assessment, Monitoring, and Enforcement activities.
 - Assure that NPCC staff is appropriately trained to conduct Certification and Auditing activities.
 - Provide detailed responses to oversight activity performed by NERC, FERC, and other relevant authorities.
 - Continue to perform and update IRAs for registered entities.
 - Continue to perform formal EIC outreach for registered entities that volunteer for such an assessment.
 - Continue to assess internal controls during monitoring engagements
 - Conduct 2021 Compliance Engagement Schedule based on budget, risk to the BPS, and number of registered entities
 - Utilize the ERO Risk-Based initiatives by:
 - Utilizing the Audit Checklist and Auditor’s Handbook for all on-site and off-site audits.
 - Preparing an updated Inherent Risk Assessment as necessary for all scheduled engagements, performing a formal Evaluation of Internal Controls for all entities that volunteer, and developing Compliance Oversight Plans (COP) for audited entities.
 - Continue to perform comprehensive enforcement investigations to determine the relevant facts and circumstances necessary to understand each noncompliance, assess the risk, and evaluate the mitigation activities or Mitigation Plan for each noncompliance. Determine the disposition method in accordance with established risk-based approaches (i.e. Compliance Exceptions, FFTs, Simplified Identification Correction Method (Québec), Settlements, etc.)
 - Evaluate the mitigation activities or Mitigation Plan for each noncompliance, track the progress and verify the completion of each Mitigation Plan.
 - As necessary, represent NPCC during any enforcement hearings before the NPCC Hearing Body, the NERC Hearing Body, the Régie, or the NBEUB.
 - Evaluate registered entities Internal Compliance Programs to determine entry into the self-logging program.
-

- Analyze noncompliance trends and associated risks in order to develop guidance to registered entities in support of a culture of reliability.
- Perform outreach (webinars, workshops) to educate entities on noncompliance root causes and on techniques for noncompliance assessment and communication associated with self-reporting to NPCC; including the provision of guidance on the development of mitigation activities that will prevent recurrence.
- Assess evolving cyber security risks for opportunities to develop internal control flow diagrams in order to provide entity guidance.

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 56% of its resources on this activity.

Resource Requirements

Personnel

- Two additional employee auditors (net increase of 1.45 FTEs after the partial re-allocation of a compliance position to IT in 2020), to increase in-house expertise rather than utilizing independent contractor labor. The increase in personnel expenses will be offset by a decrease in Consultants and Contracts.

Fixed Assets

- No new functionality is planned for the Compliance Issues Tracking System (CITS) and CMEP Data Administration Application (CDAA) at this time based on the planned implementation of the ERO Enterprise CMEP data application (Align).

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 2021 business plan are shown in the table below. Explanations of variances by expense category are included with the Supplemental Tables found in Section B.

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
Compliance Monitoring and Enforcement and Organization Registration and Certification						
	2020 Budget	2020 Projection	Variance 2020 Projection v 2020 Budget Over(Under)	2021 Budget	Variance 2021 Budget v 2020 Budget Over(Under)	
Funding						
ERO Funding						
ERO Assessments	\$ 9,034,625	\$ 9,034,625	\$ -	\$ 8,822,203	\$ (212,422)	
Penalty Sanctions	69,994	69,994	-	363,371	293,378	
Total ERO Funding	\$ 9,104,618	\$ 9,104,618	\$ -	\$ 9,185,575	\$ 80,956	
Membership Dues	-	-	-	-	-	
Testing Fees	-	-	-	-	-	
Services & Software	-	-	-	-	-	
Workshops & Misc Revenue	-	-	-	-	-	
Interest & Investment Income	-	-	-	-	-	
Total Funding (A)	\$ 9,104,618	\$ 9,104,618	\$ -	\$ 9,185,575	\$ 80,956	
Expenses						
Personnel Expenses						
Salaries	\$ 2,928,438	\$ 2,808,438	\$ (120,000)	\$ 3,058,980	\$ 130,541	
Payroll Taxes	202,717	189,717	(13,000)	214,970	12,253	
Benefits	732,104	696,104	(36,000)	834,388	102,284	
Retirement Costs	314,664	296,664	(18,000)	333,201	18,537	
Total Personnel Expenses	\$ 4,177,923	\$ 3,990,923	\$ (187,000)	\$ 4,441,539	\$ 263,616	
Meeting Expenses						
Meetings & Conference Calls	\$ 15,000	\$ 15,000	\$ -	\$ 10,000	\$ (5,000)	
Travel	300,400	300,400	-	360,000	59,600	
Total Meeting Expenses	\$ 315,400	\$ 315,400	\$ -	\$ 370,000	\$ 54,600	
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ 1,097,150	\$ 1,097,150	\$ -	\$ 707,150	\$ (390,000)	
Office Rent	-	-	-	-	-	
Office Costs	-	-	-	18,000	18,000	
Professional Services	-	-	-	-	-	
Computer & Equipment Leases	-	-	-	-	-	
Miscellaneous	-	-	-	-	-	
Total Operating Expenses, excluding Depreciation	\$ 1,097,150	\$ 1,097,150	\$ -	\$ 725,150	\$ (372,000)	
Total Direct Expenses	\$ 5,590,473	\$ 5,403,473	\$ (187,000)	\$ 5,536,689	\$ (53,784)	
Indirect Expenses	\$ 3,420,003	\$ 3,420,003	\$ -	\$ 3,597,350	\$ 177,347	
Other Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	\$ -	
Total Expenses (B)	\$ 9,010,476	\$ 8,823,476	\$ (187,000)	\$ 9,134,038	\$ 123,563	
Change in Net Assets (=A-B)	\$ 94,142	\$ 281,142	\$ 187,000	\$ 51,536	\$ (42,606)	
Fixed Asset Additions, excluding Right of Use Assets (C)	\$ 99,157	\$ 99,157	\$ -	\$ 56,551	\$ (42,606)	
TOTAL BUDGET (=B+C)	\$ 9,109,633	\$ 8,922,633	\$ (187,000)	\$ 9,190,590	\$ 80,956	
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ (5,015)	\$ 181,985	\$ 187,000	\$ (5,015)	\$ -	

Reliability Assessment and Performance Analysis Program

Reliability Assessment and Performance Analysis Program Resources			
(in whole dollars)			
	2020 Budget	2021 Budget	Increase (Decrease)
Total FTEs	5.43	5.44	0.01
Direct Expenses	\$2,169,556	\$2,320,039	\$150,483
Indirect Expenses	\$1,031,701	\$1,006,148	(\$25,553)
Other Non-Operating Expenses	\$0	\$0	\$0
Fixed Asset Additions	\$29,913	\$15,817	(\$14,096)
Total Funding Requirement	\$3,231,169	\$3,342,004	\$110,835

Program Scope and Functional Description

NPCC, through its top technical committee, the Reliability Coordinating Committee (RCC), integrates the deliverables of its Task Forces' and Working Groups' Reliability Assessment and Performance Analysis (RAPA) related activities.

Seasonal assessments of the overall NPCC resource adequacy 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 criteria 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.

2021 Key Focus Areas

In collaboration with NERC, Key Focus Area activities for 2021 include:

- Undertake special assessments and studies, including case-specific examples of real and potential impacts, to understand emerging risks from new technologies, and launch appropriate task forces to develop mitigation options. Some of these efforts may be in collaboration with state regulators, policymakers, and stakeholders, such as the National Association of Regulatory Utility Commissioners (NARUC), focusing on distributed energy resources and other risks emanating from events or conditions on the increasingly integrated distribution system that may cause cascading of the BPS.
- Integrate NERC and Regional Entity assessments to ensure that identified risks are being properly addressed, and continue to monitor those risks to understand region-specific expressions of industry-wide issues and impacts.
- Develop measures of BPS and cyber resilience, including the ability to prepare for, withstand, and recover from extreme contingencies, such as high-impact, low frequency events, and identify processes and approaches to enhance resilience through NERC's reliability and security toolkit as well as industry action. Work in collaboration with the forums and Department of Energy (DOE).

- Use data analytics, research, and relationships with other critical infrastructures to identify leading indicators of emerging risks and the potential harm of currently unknown risks, and prioritize and communicate these to industry for awareness and mitigation.
- Collaborate effectively with other non-profit organizations that share elements of the ERO Enterprise’s reliability and security mission, and seek out and work with representatives of academia, other critical infrastructures, and international experts to broaden the ERO Enterprise’s collective knowledge and awareness of current and unknown risks and strategies to address them.
- Leveraging the Regional Entity’s specialized and localized point of view, strengthen and expand outreach, coordination, and collaboration with state energy regulators and related offices to address risks to reliability stemming from the relocation of resources and interdependency between the operations of distribution and the BPS.
- Strengthen proactive outreach and communications with key provincial, federal, and state regulatory, legislative, and policy bodies and associations across North America.

Eastern Interconnection Reliability Assessment Group (ERAG)

The primary function of the Eastern Interconnection Reliability Assessment Group (ERAG) is to support 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 Committee.

NPCC RAPA staff participates with the ERAG Committee as one of the four Eastern Interconnection Regional Entities, and acts as the liaison between the ERAG Multiregional Modeling Working Group (MMWG), NPCC Reliability Coordinating Committee (RCC), NPCC Task Force on System Studies (TFSS) and the NPCC SS-37 Working Group on Base Case Development.

ERAG Committee Activities 2021 Goals and Deliverables

- Oversee the steady state and dynamic simulation base case data compilation and development.
- Oversee the ERAG assessment plan and coordinate assessment efforts with NERC Assessment Program staff. Determine the targeted ERAG assessment topic for 2021. Determine the method of assessment: analytical study, research effort, peer review.
- Make appropriate revisions, as necessary, to the ERAG Strategic Direction (i.e. anticipated new developments in MMWG process and system assessments).
- Develop and approve the ERAG activity budgets.

Multi-Regional Modeling Working Group 2021 Goals and Deliverables

- Facilitate the completion of the steady state and dynamic simulation base case data compilation and development for the 2021 series of cases.
- Check and confirm that the dynamic model data passes all applicable checks and acceptance criteria and emphasize the accurate modeling of distributed energy resources.
- Incorporate dispatch information into the future and seasonal MMWG base cases so that the dispatches are more closely aligned with economic dispatch practices.
- Continue to improve the representations of the governor-turbine plant control models.
- Apply MMWG base case non-disclosure agreement process so that MMWG cases continue to have sufficient protections in place for use and transmittal of confidential data and information.

ERAG System Assessments 2021 Goals and Deliverables

- Determine an appropriate topic of focus for the 2021 ERAG Assessment. In recent years, ERAG has conducted peer reviews on select topics in lieu of conducting assessments. Conduct the 2021 ERAG Assessment and prepare any associated documentation.
- Coordinate Assessment efforts with the NERC Reliability Assessment and System Analysis (RASA) Program staff to incorporate any risk-based or other approaches to supplement NERC Assessments.

Bulk Electric System Notification and Exception (BESnet) application and Exception Request (ERs)

NPCC supports maintenance of the BESnet application and the processing of the Regional BES Exception Requests (ERs), including periodic certifications that the basis for an Element being included or excluded in the BES through the Exception remains valid. No NPCC Exclusion Exception Requests are due for recertification in 2021. Analysis of an Exception Request from a New Brunswick entity may extend into 2021.

2021 NERC Activities

NPCC will provide the Regional perspective with appropriate NPCC RAPA staff participation on selective NERC Technical Committees and key related NERC Subcommittees, Task Forces and Working Groups, including:

- Inverter-Based Resource Performance Task Force (IRPTF)
- Performance Analysis Subcommittee (PAS)
 - Demand Response Availability Data System Working Group (DADSWG)
 - Generating Availability Data System Working Group (GADSWG)
 - Misoperation Information Data Analysis System Working Group (MIDASWG)
 - Transmission Availability Data System Working Group (TADSWG)
- Reliability Assessment Subcommittee (RAS)
 - Probabilistic Assessment Working Group (PAWG)
- System Analysis and Modeling Subcommittee (SAMS)
 - Load Modeling Task Force (LMTF)
 - Power Plant Model Verification Task Force (PPMVTF)
 - Node Breaker Modeling Group (NBMG)
- System Protection and Control Subcommittee (SPCS)
- Synchronized Measurement Subcommittee (SMS)
- System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG)
- ERO RAPA Steering Group (ERO RAPA-SG)
 - Reliability Assessment Ad Hoc Team
 - Performance Analysis Ad Hoc Team
 - Event Analysis Ad Hoc Team
 - Situational Awareness Ad Hoc Team
 - System Analysis Ad Hoc Team

ERO – Operations Leadership Team (OLT) 2021 Activities

- Provide analytic support for the ERO Executive Committee;
- Bulk Electric System Exception Process and BES Definition sub-team, under Organization Registration and Certification Group (ORCG);

- ERO-RAPA Group; and,
- Other activities as directed by the ERO Executive Committee.

2021 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 the reliable and efficient planning of the international interconnected bulk power systems in Northeastern North America through the coordination of NPCC Balancing Authority or Control Area (Area) and NERC planning processes and activities.

TFCP Reliability Assessment and Performance Analysis 2021 Goals and Deliverables

- Coordinate the NPCC Area reviews in accordance with the requirements of NPCC Directory No. 1, “Design and Operation of the Bulk Power System.”
- Oversee the NPCC Directory No. 1 Implementation Plan (Dated: September 30, 2015).
- Coordinate the review of proposed new, modified and retired remedial action schemes (RAS) in accordance with the NPCC Directory No. 7, “Procedure for Review of System Special Protection Systems.”
- Coordinate the development of additional NPCC Criteria, as necessary, and track any new and developing Regional NPCC Standards through the NPCC Regional Standards Committee.
- Monitor industry practices and make recommendations to the NPCC Regional Standards Committee regarding related NERC Standards.
- Oversee the activities of the NPCC CP-8 Working Group.
- Evaluate and recommend RCC approval of NPCC Area Transmission Reviews.
- Evaluate and recommend RCC approval of NPCC Area Reviews of Resource Adequacy.
- Conduct, through the CP-8 Working Group, the 2021 NPCC Tie Benefit Study.
- Coordinate the NPCC transition from SPS to RAS.
- Lead the NPCC Task Forces in conducting the review of the reliability and cost benefit of Directory No. 1, Design and Operation of the BPS.
- Support related reliability activities, including consideration of any requests for sub-regional assessments.
- Keep informed on studies and developments in neighboring systems which might impact NPCC reliability.
- Assess use of emerging technologies for consistency with current best reliability practices.
- Review Events Analysis Lessons Learned using the Events Analysis discussion/review template.
- Review the load shape assumption through the CP-8 Working Group used in NPCC Multi-Area probabilistic reliability Assessments.
- Monitor the reliability issues associated with fuel supply, demand resources, energy efficiency, and conservation methods including all intermittent renewable resources and distributed energy resources.

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 international interconnected bulk power systems in Northeastern North America and for the review of related NPCC documents.

TFSS Reliability Assessment and Performance Analysis 2021 Goals and Deliverables

- Review and recommend approval of Area Transmission Reviews.
- Review and classify new and modified Remedial Action Schemes.
- Review and Implement the NPCC A-10 Criteria.
- Perform annual review and update of the Major Project List.
- Participate in the development and submission of NPCC comments/inputs into the development of regional and/or continent-wide reliability standards that address the NERC Reliability Standards.
- Provide support and technical input, for Task Force related Bulk Electric System risks as identified by the NERC Reliability Issues Steering Committee.
- Review existing NPCC Regional Criteria and procedures for validation of data used in power flow and dynamic simulations; propose changes to provide for adequate data validation.
- Perform investigation of Distributed Energy Resources modeling practices.
- Annually develop a library of power flow base cases and associated dynamic cases.
- Enable the annual review of the NPCC event replication procedure and ensure the preparedness of the NPCC Planning Coordinators to develop base cases for a required investigation of a major system event in or affecting NPCC and support the performance of event replication by benchmarking simulations against actual system performance.
- Work with software vendors and NERC to enhance the capability for dynamic simulations.
- Continue to investigate the use of dynamic load models for transient stability studies.
- Investigate the use of load monitoring equipment to aid in the benchmarking of dynamic load models used in transient stability studies.

Task Force on System Protection

The primary purpose of the NPCC Task Force on System Protection (TFSP) is to promote the reliable and efficient operation of the international interconnected bulk power systems in Northeastern North America through the establishment of directories, criteria, guidelines, and procedures and coordination of design, relative to NPCC protection systems.

TFSP Reliability Assessment and Performance Analysis 2021 Goals and Deliverables

- Assess proposed protection systems and remedial action schemes.
- Participate and/or serve as lead Task Force in the implementation of applicable Regional NERC Reliability Standards.
- Review and respond to Questions, Requests for Interpretations and/or Clarifications related to bulk power system protection requirements in NPCC Directories and Criteria.
- Participate in the ongoing development and submission of NPCC inputs/comments into the development of related NERC Reliability Standards.
- Manage the misoperations review and analysis of transmission and generation protection systems.
- Monitor the NPCC metric on protection system Misoperation Risk Index Score calculations.

- Review mitigations and/or progress reports for Bulk Power System Risk Reduction Implementation.
- Provide support and technical input for related protection system risks as identified by the NERC Reliability Issues Steering Committee.
- Conduct review/development of related NPCC Directories.
- Consistent with the TFSP's scope, conduct joint meeting with other Regions to share best practices and experiences.
- Review ongoing changes to the North American Reliability Corporation Critical Infrastructure Protection Standards and evaluate impacts to Registered Entities Protection Systems, SCADA, and Monitoring Systems.

Task Force on Coordination of Operation

The NPCC Task Force on Coordination of Operation (TFCO) primarily facilitates the coordination of operations among the NPCC Reliability Coordinator areas and adjacent NERC Regions to enhance the reliability of the bulk power system.

TFCO Reliability Assessment and Performance Analysis 2021 Goals and Deliverables

- Prepare and conduct the spring and autumn NPCC System Operator Seminars.
- Develop and securely disseminate the annual compilation of "Facilities for Notification."
- On a biennial basis, perform a voluntary Critical Operating Tool Analysis Survey accompanied with the previous surveys recommendation to disseminate and assess the implementation of best practices and recommendations.
- Support an annual enhanced, wide-area restoration drill among the Reliability Coordinator areas of NPCC and their neighboring Reliability Coordinators incorporating the annual review of the NPCC regional restoration plan.
- Support and take part in a biennial, continent-wide Grid Security Exercise (GridEx), including a review of the associated reports and Lessons Learned.
- Monitor and discuss the trends and impacts of the changing resource mix (including intermittent, DER, batteries, etc.) and the effects of the proliferation of the new resources on real-time operations, as well as behavior during and impacts on recovery and restoration plans.
- Review and analyze the performance of Simultaneous Activation of Reserve (SAR) implementation following an event to enhance the process.
- Conduct seasonal NPCC Reliability Assessment and incorporate the multi-area probabilistic simulation results in each assessment. Coordinate the NPCC input for the annual short-term NERC Reliability Assessment Subcommittee assessment.
- Develop respective scopes for and conduct reviews of applicable NPCC Directories, Criteria, Guides and Procedures in accordance with their applicable review dates.
- Assess the current capabilities of system operations communication systems.
- Evaluate practices, procedures and capabilities of system operators in detection and operational response to potential cyber security incidents, as well as notification and coordination practices and capabilities among NPCC and neighboring system operators in response to cyber intrusion into operations systems.

NPCC Regulatory/Governmental Affairs Advisory Group

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 reliability matters. A related contributing activity is to strengthen proactive outreach and communication with key provincial, federal, state regulatory, legislative, and policy bodies and associations across North America.

NPCC Regulatory/Governmental Affairs Advisory Group 2021 Goals and Deliverables

- Continued outreach to NPCC’s state electricity and environmental regulators stressing the importance of understanding and considering reliability impacts during the development of State/Provincial initiatives (such as the identified Essential Reliability Services, Distributed Energy Resource integration).
- Focus on initiatives concerning regional planning, distributed energy resource requirements, the timing of new generation resources and transmission infrastructure projects.

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% of its resources on these activities.

Resource Requirements

Personnel

- No significant changes.

Consultants and Contracts

- Increase in consultants and contracts expense is associated with increase in inherent risk and emerging risk reliability assessments.

Reliability Assessment and Performance Analysis Program

Funding sources and related expenses for the Reliability Assessment and Performance Analysis section of the 2021 business plan are shown in the table below. Explanations of variances by expense category are included with the Supplemental Tables found in Section B.

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
Reliability Assessment and Performance Analysis						
	2020 Budget	2020 Projection	Variance 2020 Projection v 2020 Budget Over(Under)	2021 Budget	Variance 2021 Budget v 2020 Budget Over(Under)	
Funding						
ERO Funding						
ERO Assessments	\$ 3,210,055	\$ 3,210,055	\$ -	\$ 3,240,373	\$ 30,318	
Penalty Sanctions	21,115	21,115	-	101,632	80,517	
Total ERO Funding	\$ 3,231,169	\$ 3,231,169	\$ -	\$ 3,342,004	\$ 110,835	
Membership Dues	-	-	-	-	-	
Testing Fees	-	-	-	-	-	
Services & Software	-	-	-	-	-	
Workshops & Misc Revenue	-	-	-	-	-	
Interest & Investment Income	-	-	-	-	-	
Total Funding (A)	\$ 3,231,169	\$ 3,231,169	\$ -	\$ 3,342,004	\$ 110,835	
Expenses						
Personnel Expenses						
Salaries	\$ 1,006,128	\$ 1,006,128	\$ -	\$ 1,017,371	\$ 11,243	
Payroll Taxes	64,023	64,023	-	64,068	46	
Benefits	218,787	218,787	-	280,566	61,779	
Retirement Costs	109,418	109,418	-	110,034	616	
Total Personnel Expenses	\$ 1,398,356	\$ 1,398,356	\$ -	\$ 1,472,039	\$ 73,683	
Meeting Expenses						
Meetings & Conference Calls	\$ 22,000	\$ 22,000	\$ -	\$ 18,000	\$ (4,000)	
Travel	216,200	216,200	-	180,000	(36,200)	
Total Meeting Expenses	\$ 238,200	\$ 238,200	\$ -	\$ 198,000	\$ (40,200)	
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ 533,000	\$ 533,000	\$ -	\$ 647,000	\$ 114,000	
Office Rent	-	-	-	-	-	
Office Costs	-	-	-	3,000	3,000	
Professional Services	-	-	-	-	-	
Computer & Equipment Leases	-	-	-	-	-	
Miscellaneous	-	-	-	-	-	
Total Operating Expenses, excluding Depreciation	\$ 533,000	\$ 533,000	\$ -	\$ 650,000	\$ 117,000	
Total Direct Expenses	\$ 2,169,556	\$ 2,169,556	\$ -	\$ 2,320,039	\$ 150,483	
Indirect Expenses	\$ 1,031,701	\$ 1,031,701	\$ -	\$ 1,006,148	\$ (25,553)	
Other Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	\$ -	
Total Expenses (B)	\$ 3,201,257	\$ 3,201,257	\$ -	\$ 3,326,188	\$ 124,931	
Change in Net Assets (=A-B)	\$ 29,913	\$ 29,913	\$ -	\$ 15,817	\$ (14,096)	
Fixed Asset Additions, excluding Right of Use Assets (C)	\$ 29,913	\$ 29,913	\$ -	\$ 15,817	\$ (14,096)	
TOTAL BUDGET (=B+C)	\$ 3,231,169	\$ 3,231,169	\$ -	\$ 3,342,004	\$ 110,835	
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ 0	\$ 0	\$ -	\$ -	\$ 0	

Training, Education, and Operator Certification Program

Training, Education, and Operator Certification Program Resources			
(in whole dollars)			
	2020 Budget	2021 Budget	Increase (Decrease)
Total FTEs	0.10	0.10	0.00
Direct Expenses	\$219,862	\$229,835	\$9,973
Indirect Expenses	\$19,000	\$18,495	(\$505)
Other Non-Operating Expenses	\$0	\$0	\$0
Inc(Dec) in Fixed Assets	\$551	\$291	(\$260)
Total Funding Requirement	\$239,412	\$248,621	\$9,209

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. NPCC staff training and development is incorporated within each respective program area.

Training Program Background and Description

This NPCC Program establishes and coordinates training for system operators relating to inter-Reliability Coordinator area matters, criteria, terminology, standards and operating procedures and instructions. It includes development and execution of training seminars, held twice yearly, at which:

- potential operational problems for the coming season are discussed,
- physical layouts and electrical characteristics of the NPCC and PJM Areas are discussed,
- application of NPCC Directory and NERC Standard requirements pertinent to operation are discussed,
- major industry issues that are important for system operators are discussed,
- significant disturbances are reviewed for lessons 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 and PJM Reliability Coordinator (RC) Areas and the Nova Scotia Balancing Authority (BA) area, as well as Newfoundland and Labrador Hydro (NLH) Energy Control Center operations. PJM RC has significant interaction with the NPCC RCs and system operators from PJM have been regular participants at past seminars. With the completion of the DC links connecting Newfoundland and Labrador Hydro to the Quebec and Eastern Interconnections, NLH has been increasing their engagement with NPCC, including active participation in the system operator seminars. Examples of specific topics addressed at recent seminars include: 1) additions and impacts to operations of renewable resources, 2) the development of conditions and violations related to major system Blackouts, 3) human performance related to system operations, 4) cybersecurity threats and system operator concerns, 5) system restoration approaches and tie-ins to neighboring systems and 6) application of NPCC Simultaneous Activation of Reserve. Usually, control center visits are included as part of the seminar activities.

This Program also provides for:

- sharing of RC/BA existing training program and system simulator area content;
- verification and sharing of training methods;
- evaluation of training and simulator aids as they become available;
- opportunities to consolidate training among the NPCC RCs and BAs, which includes opportunities to share training material and training sessions; and
- exchange of information on internal methods of system operator training.

2021 Key Long-Term Focus Areas

ERO Enterprise Long-Term Strategy Focus Area activities for 2021 include:

- Build appropriate outreach, training, and education to registered entities through NERC and the Regional Entities to reduce the incidence of known risks to reliability;
- Nurture relationships with key industry trade associations, as well as those associations representing technology, affiliated sectors, and end users to understand context and leverage their experience and reach;
- Collaborate effectively with other non-profit organizations that share elements of the ERO Enterprise’s reliability and security mission, and seek out and work with representatives of academia, other critical infrastructures, and international experts to broaden the ERO Enterprise’s collective knowledge and awareness of current and unknown risks and strategies to address them;

2021 NERC Activities

NPCC will provide the Regional perspective and support with appropriate NPCC Training and Education staff participation on selective NERC Committees, including:

- ERO Enterprise and NATF Electric Power Human Performance Improvement Symposium (EPHPIS) Organizing Committee
- Reliability Training Working Group (RTWG)

Activities below further support the NPCC 2020-23 Strategic Plan through targeted discussion of operational impacts and considerations in the specific Focus Areas, including:

- Critical infrastructure interdependencies
- DERs
- Identifying and collaboratively advancing better practices to mitigation of security threats

Funding Drivers and Reliability Benefits

- System operators participating in the Seminars: 1) share various approaches to addressing operational problems and learn about the characteristics of neighboring systems; 2) gain exposure to NPCC issues and current industry operational topics; 3) review recent NPCC and PJM major external disturbances; 4) review key operational related content in NPCC Directories and NERC Standards; and 5) participate in hands-on “table top exercises” pertaining to system operational practices. PJM system operators and trainers are also invited to participate and normally attend and participate in these seminars;

- Seminar attendees also receive Continuing Education Hours (CEHs) (normally 3 CEHs) and operator trainers from each RC/BA area can utilize the seminar content by including it in their internal training programs to provide CEHs to all system operators; The seminars help to improve system operational coordination through better contact among system operators at other Reliability Coordinator Areas.
- Continually review and revise the curriculum of the training seminars to better emphasize NERC Standard requirements related to system operation, NPCC wide-area operations and Regionally-specific criteria and procedures.
- Enhance system operator awareness and knowledge of the standards, criteria and procedures that are applied in real time operation;
- Provide more sharing of 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 RC/BA areas:
- Provide a forum among NPCC RC/BA areas for sharing of approaches to meet the requirements of the NERC PER and COM standards;
- NPCC will conduct two Standards and Compliance workshops in 2020, 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).

2021 Key Assumptions

In addition to the Spring and Fall Standards and Compliance workshops, NPCC regularly conducts System Operators seminars, specifically designed with table top exercises, targeted breakout classroom sessions and presentations on current industry related activities, to provide for the most efficient exchange of information between the NPCC and Areas' training staff, 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 and Areas' training staff members. To supplement these seminars and workshops, NPCC may develop webinars that will focus on specific topics pertinent to developments related to system operations, compliance program implementation, standards development or technical issues.

The System Operator seminars involve system operators' participants from the NPCC RC/BA Areas and PJM, as well as Newfoundland and Labrador Hydro, and are held in early May and early November.

Additionally, NPCC staff participates on the ERO Enterprise and NATF Electric Power Human Performance Improvement Symposium (EPHPIS) Organizing Committee, members of which include the Regions and NERC, along with the NATF and is charged with executing the administrative framework for organizing, planning and implementing the event is collaborative in nature. EPHPIS is a continent-wide collaboration between the ERO Enterprise and the North American Transmission Forum (NATF) focused on human performance improvement for the bulk power system (BPS).

Training, Education and Operator Certification 2021 Goals and Deliverables

- Prepare and conduct the 2021 Spring and Fall NPCC System Operator Seminars.
- Continue collaboration and sharing of the intended RC/BA approaches, experiences and materials to task identification and training development

-
- As needed, enhance the 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 Standards PER-003-1 “*Operating Personnel Credentials*” and PER-005-2 “*Operations Personnel Training*.”
 - Develop on-line operational training webinars that focus on specific topics pertinent to compliance program implementation, standards development or technical issues.
 - Conduct Spring and Fall 2021 Standards and Compliance workshops addressing the development of NERC and Regional Reliability Standards and the implementation of the Compliance Monitoring and Enforcement Program (CMEP).
 - Support EPHPIS Organization Committee activities and execution of the HP symposium.
 - Participate on the Reliability Training WG and collaborate with the NPCC CO-2 Operations Training WG and other NPCC Members’ training personnel on the activities related to the reliable operation of the BES.

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 2% of its resources on this activity.

Resource Requirements

- No significant changes.

Training, Education, and Operator Certification Program

Funding sources and related expenses for the training, education, and operator certification section of the 2021 business plan are shown in the table below. Explanations of variances by expense category are included with the Supplemental Tables found in Section B.

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
Training, Education, and Operator Certification						
				Variance		Variance
	2020	2020	2020 Projection	2020 Projection	2021	2021 Budget
	Budget	Projection	v 2020 Budget	Over(Under)	Budget	v 2020 Budget
				Over(Under)		Over(Under)
Funding						
ERO Funding						
ERO Assessments	\$ 171,524	\$ 171,524	\$ -		\$ 179,253	\$ 7,729
Penalty Sanctions	389	389	-		1,868	1,479
Total ERO Funding	\$ 171,912	\$ 171,912	\$ -		\$ 181,121	\$ 9,209
Membership Dues	-	-	-		-	-
Testing Fees	-	-	-		-	-
Services & Software	-	-	-		-	-
Workshops & Misc Revenue	67,500	33,750	(33,750)		67,500	-
Interest & Investment Income	-	-	-		-	-
Total Funding (A)	\$ 239,412	\$ 205,662	\$ (33,750)		\$ 248,621	\$ 9,209
Expenses						
Personnel Expenses						
Salaries	\$ 11,793	\$ 11,793	\$ -		\$ 18,352	\$ 6,559
Payroll Taxes	939	939	-		1,068	129
Benefits	5,652	5,652	-		6,091	440
Retirement Costs	1,478	1,478	-		2,324	846
Total Personnel Expenses	\$ 19,862	\$ 19,862	\$ -		\$ 27,835	\$ 7,973
Meeting Expenses						
Meetings & Conference Calls	\$ 185,000	\$ 120,000	\$ (65,000)		\$ 191,000	\$ 6,000
Travel	15,000	15,000	-		11,000	(4,000)
Total Meeting Expenses	\$ 200,000	\$ 135,000	\$ (65,000)		\$ 202,000	\$ 2,000
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ -	\$ -	\$ -		\$ -	\$ -
Office Rent	-	-	-		-	-
Office Costs	-	-	-		-	-
Professional Services	-	-	-		-	-
Computer & Equipment Leases	-	-	-		-	-
Miscellaneous	-	-	-		-	-
Total Operating Expenses, excluding Depreciation	\$ -	\$ -	\$ -		\$ -	\$ -
Total Direct Expenses	\$ 219,862	\$ 219,862	\$ (65,000)		\$ 229,835	\$ 9,973
Indirect Expenses	\$ 19,000	\$ 19,000	\$ -		\$ 18,495	\$ (505)
Other Non-Operating Expenses	\$ -	\$ -	\$ -		\$ -	\$ -
Total Expenses (B)	\$ 238,862	\$ 238,862	\$ (65,000)		\$ 248,330	\$ 9,469
Change in Net Assets (=A-B)	\$ 551	\$ (33,199)	\$ 31,250		\$ 291	\$ (260)
Fixed Asset Additions, excluding Right of Use Assets (C)	\$ 551	\$ 551	\$ -		\$ 291	\$ (260)
TOTAL BUDGET (=B+C)	\$ 239,412	\$ 239,412	\$ (65,000)		\$ 248,621	\$ 9,209
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ 0	\$ (33,750)	\$ 31,250		\$ -	\$ (0)

Situation Awareness and Infrastructure Security Program

Situation Awareness and Infrastructure Security Program Resources (in whole dollars)			
	2020 Budget	2021 Budget	Increase (Decrease)
Total FTEs	5.40	5.40	0.00
Direct Expenses	\$1,450,129	\$1,447,759	(\$2,370)
Indirect Expenses	\$1,026,001	\$998,750	(\$27,251)
Other Non-Operating Expenses	\$0	\$0	\$0
Fixed Asset Additions	\$29,747	\$15,701	(\$14,047)
Total Funding Requirement	\$2,505,877	\$2,462,210	(\$43,668)

Program Scope and Functional Description

The Situation Awareness and Infrastructure Security (SAIS) 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 an event does occur, it is critical to provide a forum for active coordination of reliability and operation among the NPCC Reliability Coordinator areas and neighboring NERC Regions and to use an event as a learning opportunity to enhance the reliability of the interconnected bulk power system through the lessons learned, which can be gleaned from such an event.

NPCC's Event Analysis Program resides within the SAIS program area and supports the overall goal of promoting the reliability of the bulk power system in Northeastern North America and the entire North American grid. NERC, Regions and the industry analyze events, identify the lessons to be learned, and conduct a formal cause code analysis. The Event Analysis Program recognizes that many events, which occur on the bulk power system beyond those identified through NERC Reliability Standard EOP-004, "Event Reporting," can have varying levels of significance to the electric system. By implementing a "bottom-up" approach to an event review within the framework of the NERC Event Analysis Program consistency, comparability, flexibility, quality and timeliness in the event analysis process will be promoted by NPCC, the registered entities and NERC in a collaborative initiative, resulting in industry lessons learned and trends identify and prioritizing possible reliability concerns.

2021 Key Focus Areas

NPCC SAIS activities will be in support of the ERO Enterprise Long-Term Strategy Focus Areas for 2021, including:

- Use the full suite of tools, activities and resources for risk mitigation to provide guidance to industry as to how to mitigate emerging risks, evaluating the effectiveness of such approaches;
- Build/enhance appropriate outreach, training, and education to registered entities to reduce the incidence of known risks to reliability;

- Develop measures of BPS and cyber resilience, and identify processes and approaches to enhance resilience through NERC’s reliability and security toolkit as well as industry action. Work in collaboration with the forums and Department of Energy (DOE);
- Strengthen the analysis of cyber impacts on the BPS and mitigate impacts of cyberattacks. Enhance industry’s ability to develop approaches to pre-position the system when under attack and explore recovery strategies;
- Leverage information and cross-sector collaboration with other critical infrastructures to identify leading indicators of emerging risks and the potential harm of currently unknown risks, and prioritize and communicate these to industry for awareness and mitigation;
- Build appropriate outreach, training, and education to registered entities through NERC and the Regional Entities to reduce the incidence of known risks to reliability;
- Ensure the E-ISAC Long-Term Strategic Plan is executed such that the E-ISAC is viewed by industry as meeting its needs as one of its key trusted sources of security information
- Collaborate with other sectors’ security infrastructure where appropriate (e.g., the Financial Systemic Analysis and Resilience Center and the Downstream Natural Gas Information Sharing and Analysis Center) to facilitate cross-sector information sharing and threat analysis;
- Strengthen proactive outreach, communications, relationships and intelligence sharing with key regulatory, legislative, and policy bodies as well as government agencies across North America (US and Canada).
- Nurture relationships with key industry trade associations, as well as those associations representing technology, affiliated sectors, and end users to understand context and leverage their experience and reach;
- Collaborate effectively with other non-profit organizations, other critical infrastructure experts that share elements of the ERO Enterprise’s reliability and security mission, and to broaden the ERO Enterprise’s collective knowledge and awareness of current and unknown risks and strategies to address them; and
- Leveraging the Regional Entities’ specialized and localized point of view, strengthen and expand outreach, coordination, and collaboration with state energy regulators and related offices to address risks to reliability stemming from the relocation of resources and interdependency between the operations of distribution and the BPS;

2021 NERC Activities

NPCC will provide the Regional perspective and support with appropriate NPCC SAIS and EA staff participation on selective NERC Committees, including:

- Event Analysis Subcommittee (EAS)
- Event Analysis Ad Hoc Team
- Situational Awareness Ad Hoc Team
- NERC Physical Security Advisory Group (PSAG)
- Grid Exercise Working Group (GridEx WG)

Activities below further support the NPCC 2020-23 Strategic Plan through targeted discussion of operational impacts and considerations in the specific Focus Areas, including targeted activities, such as:

- Enhancing System Resilience and Assuring Energy Sufficiency
 - Gathering and trending analytical data related to system resilience and identifying better practice elements for BPS reliability

- o Developing resilience metrics to better quantify the reliability enhancements of prevent operations in a more secure state, reductions in the system degradation profile, and increasing the speed of recovery
 - o Assessing gas-electric interdependencies, as well as other common mode failure and single points of disruption scenarios involving communications, water, and other interdependent critical infrastructure sectors
- Addressing Cyber and Physical Threats
 - o Developing Regional concurrence on appropriate levels of cyber resilience, the adequacy of security controls, and methodologies to simulate cyber impacts on BPS reliability
 - o Expanding Regional support for and interaction with the E-ISAC and enhancing actionable information sharing within Northeastern North America
 - o Identifying and collaboratively advancing better practice approaches to mitigating cyber and physical security threats

2021 Key Assumptions

- The monitoring of Lessons Learned will continue to be a major focus of NERC and NPCC in 2021, including:
 - o continued reporting, for applicable qualifying events in the voluntary Event Analysis Program, of more detailed information on station equipment failure, per recommendation of the AC Substation Equipment Task Force, to solicit and collect this data, to aid in future analysis of station equipment failures and to identify trends that may be a threat to the reliability of the Bulk Electric System,
 - o Introduction of a new EAP categories, implemented to capture the effect of “non-consequential” loss of inverter type resources and similarly DC ties between two separate asynchronous systems,
 - o continued utilization of a revised Category 1h - EMS/Loss of monitoring or control at a Control Center events Brief Report template and Addendum, developed with the input of the EMS Working Group to ensure continuation of analysis of such events to improve information collection related to such events and associated analysis, taking into account the modifications to the mandatory EOP-004-4 reporting requirements thresholds.
- TFIST support of the following activities:
 - o Supply Chain – new version of the Standard, more guidelines by RSTC’s Supply Chain WG and industry (like NATF)
 - o Virtualization – updates to several CIP Standards
 - o IEC 61850 – addressing a gap in cyber security because it is excluded from CIP
 - o CIP-012 implementation
 - o CIP-008 – new version which requires notifying E-ISAC and United States National Cybersecurity and Communications Integration Center (NCCIC)
 - o IST-4 WG – patch management of relays
 - o Grid Ex VI (2021)
 - o BES Cyber Systems Information (BCSI) - CIP updates approval and entities’ implementation

- Resource allocation to this program area supports expanded Events Analysis activities; coordination with NERC’s evolving E-ISAC capabilities; and physical and cyber security outreach efforts, including support of NERC’s Security Initiative and cross-sector collaboration activities.
- Support DOE-led effort on the development of the North American Energy Resilience Model (NAERM) in collaboration with the National Labs, the industry and the ERO Enterprise
- Further activities in the cross-sector interdependencies, including natural gas and communications

Situation Awareness 2021 Goals and Deliverables

- NPCC will provide the Regional perspective through NPCC staff support of the NERC Reliability and Security Technical Committee and participation on the key related NERC Subcommittees, Task Forces and Working Groups, including the Event Analysis Subcommittee, the ERO – Event Analysis and Situational Awareness Group.
 - Work directly with applicable NPCC Task Forces and Working Groups to provide an in-depth assessment of Lessons Learned unique to the NPCC Members and NPCC Criteria.
 - Situation Awareness:
 - Monitor the operational status of the bulk power system and coordinate normal and pre-emergency communication, awareness and assistance in addition to the same during an emergency among the Reliability Coordinators within 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.
 - Prepare daily reports and conduct daily and weekly conference calls to serve as a complement to the NPCC Emergency Preparedness Conference Call. The participants of the calls are the Reliability Coordinators within NPCC and its neighboring RCs, the Midcontinent ISO and PJM.
 - Monthly test of the satellite telephone network, to ensure the capability for continued voice communications among NPCC and its Reliability Coordinators.
 - Monthly test of the NPCC Emergency Preparedness Communications Procedure, as required
 - Coordination and communication with the NERC Bulk Power System Awareness group in preparation for and during ongoing significant events in the NPCC’s footprint;
 - Participation in the ERO Enterprise-wide Situation Awareness activities, including NERC SA Oversight Plan specified goals and deliverables in support of the activities to identify, prioritize, and assure effective and efficient mitigation of risk to the reliability and security of the North American Bulk Power System (BPS).
 - Monitor the status of the bulk power system through the NERC Situational Awareness-FERC, NERC, Regions version 3 (SAFNRv3) tool
 - Coordinating inter-Regional pre-emergency actions in the event of a threat to the security of the Northeastern North American bulk power supply system.

- o Assisting in the development and performance of real-time operating tools ensuring cyber security concerns are addressed.
 - o Take part in planning activities and distributed play portion of the GridEx VI wide-area exercise, including incorporating and building on Lessons Learned from the GridEx V event and develop new lessons learned.
- Events Analysis:
 - o Continue to promote, implement and manage voluntary ERO Event Analysis Process (EAP) and Cause Coding process as part of the ERO Event Analysis Program, including review and analysis of applicable, qualifying events, development of lessons learned and cause coding of events.
 - o Promote NPCC's Event Analysis group's process for sharing and dissemination of the detailed Event Analysis Report information among industry participants (registered entities).
 - o Participation in the ERO Enterprise-wide Events Analysis activities, including NERC EA Oversight Plan specified goals and deliverables in support of the activities to identify, prioritize, and assure effective and efficient mitigation of risk to the reliability and security of the North American Bulk Power System (BPS).
 - o Work directly with applicable NPCC Task Forces and Working Groups to provide an in-depth assessment of Lessons Learned unique to the NPCC Members and NPCC Criteria and development of Regional Insights, as applicable.
 - o Support ERO Enterprise lessons learned development through participation on the NPCC events lessons learned review teams, as well as lessons learned from other Regions and NERC.

Infrastructure Security Objectives

NPCC's critical infrastructure security objectives are defined within the scope of the NPCC Task Force on Infrastructure Security & Technology, and include, but are not limited to:

- Providing a forum for NPCC review of proposed and posted documents from the NERC Critical Infrastructure Protection Committee; and,
- 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 physical and cyber security outreach efforts, will supplement infrastructure security focus areas and support the ERO Enterprise contributing activity of "Strengthen relationships and intelligence sharing with key government agencies, such as the DOE as the U.S. electricity sector-specific agency, the Department of Homeland Security (DHS), as well as Natural Resources Canada (NRCan), Canada's Communications Security Establishment" and "Build appropriate outreach, training, and education to registered entities through NERC and the Regional Entities to reduce the incidence of known risks to reliability" as it pertains to the operational security (both cyber and physical).

NPCC's Physical Security Working Group – an NPCC group of physical security experts formed to discuss, in a secure environment, emerging threats, trends and new security technologies and strategies utilized by NPCC registered entities for the protection of their facilities in the physical arena. The Working Group is tasked with developing approaches to physical security that will enhance the reliability and resiliency of the BPS and further address any physical security issues that could challenge efficient operation of the BPS, including pertinent items identified in the

biennial RISC report, under Physical and Cyber Security Vulnerabilities. The Group will function as a clearinghouse for intelligence information received from Federal, State and Local partners and will disseminate such information received to NPCC registered entities. In addition, the Working Group shall develop, review, and provide regional input on various industry physical security initiatives, working groups, and task forces, as appropriate.

Infrastructure Security 2020 Goals and Deliverables

- Monitor the reliable implementation of the Cyber Security Standards.
- Monitor the Homeland Security Information Network (HSIN), E- ISAC, NERC Alerts and Canadian Information Sharing and share information with the NPCC CO-8 Working Group, NPCC PSWG and NPCC members' cyber security experts.
- 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.
- Provide support and technical input for TFIST and PSWG related to the Bulk Power System risks as identified by the NERC Reliability Issues Steering Committee; support, discuss and coordinate activities and approaches identified in the recommendations for mitigating security risks.
- Support the NERC Grid Exercise Working Group in GridEx VI planning, simulation and after-action report development portions of the exercise.
- Review infrastructure security & technologies and provide recommendations to enhance physical and cyber security in compliance with NERC guidelines/standards.
- Provide recommendations to enhance physical and cyber security, in compliance with NERC standards, based on assessments of available and emerging infrastructure security technologies, methodologies, and best practices.
- Sponsor periodic workshop presentations to address timely issues and update NPCC Members associated with infrastructure security and technology.
- Provide education, awareness, and support for Cross Sector coordination in Entity agreements and response plans with focus upon Telecommunications, Water and Natural Gas, including monitoring and sharing with the E-ISAC.
- Provide physical and cyber security outreach services to registered entities.
- Support ERO Enterprise Security Initiative and grow coordination and collaboration with the ERO, E-ISAC, other NERC Regions and US and Canadian federal, state and local Authorities.
- Facilitate and provide coordination and technical support and guidance to the NPCC Physical Security Work Group; share and collaborate with other Regions and NERC on good industry practices to enhance security posture.
- Conduct an annual review of cross border emergency telecommunications to verify each Area can communicate with each other.
- Provide a forum for members of NPCC, NPCC Task Forces and Working Group to identify and discuss cyber security issues and practices related to the bulk power system.

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 15% of its resources on this activity.

Resource Requirements

- No significant changes.

Situation Awareness and Infrastructure Security Program

Funding sources and related expenses for the situation awareness and infrastructure security section of the 2021 business plan are shown in the table below. Explanations of variances by expense category are included with the Supplemental Tables found in Section B.

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
Situation Awareness and Infrastructure Security						
	2020 Budget	2020 Projection	Variance 2020 Projection v 2020 Budget Over(Under)	2021 Budget	Variance 2021 Budget v 2020 Budget Over(Under)	
Funding						
ERO Funding						
ERO Assessments	\$ 2,484,879	\$ 2,484,879	\$ -	\$ 2,361,325	\$ (123,554)	
Penalty Sanctions	20,998	20,998	-	100,885	79,887	
Total ERO Funding	\$ 2,505,877	\$ 2,505,877	\$ -	\$ 2,462,210	\$ (43,668)	
Membership Dues	-	-	-	-	-	
Testing Fees	-	-	-	-	-	
Services & Software	-	-	-	-	-	
Workshops & Misc Revenue	-	-	-	-	-	
Interest & Investment Income	-	-	-	-	-	
Total Funding (A)	\$ 2,505,877	\$ 2,505,877	\$ -	\$ 2,462,210	\$ (43,668)	
Expenses						
Personnel Expenses						
Salaries	\$ 924,110	\$ 884,110	\$ (40,000)	\$ 885,454	\$ (38,656)	
Payroll Taxes	61,713	57,713	(4,000)	60,515	(1,198)	
Benefits	202,020	190,020	(12,000)	233,918	31,898	
Retirement Costs	99,986	93,986	(6,000)	96,873	(3,113)	
Total Personnel Expenses	\$ 1,287,829	\$ 1,225,829	\$ (62,000)	\$ 1,276,759	\$ (11,070)	
Meeting Expenses						
Meetings & Conference Calls	\$ 8,000	\$ 8,000	\$ -	\$ 8,000	\$ -	
Travel	94,300	94,300	-	110,000	15,700	
Total Meeting Expenses	\$ 102,300	\$ 102,300	\$ -	\$ 118,000	\$ 15,700	
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ 60,000	\$ 60,000	\$ -	\$ 50,000	\$ (10,000)	
Office Rent	-	-	-	-	-	
Office Costs	-	-	-	3,000	3,000	
Professional Services	-	-	-	-	-	
Computer & Equipment Leases	-	-	-	-	-	
Miscellaneous	-	-	-	-	-	
Total Operating Expenses, excluding Depreciation	\$ 60,000	\$ 60,000	\$ -	\$ 53,000	\$ (7,000)	
Total Direct Expenses	\$ 1,450,129	\$ 1,388,129	\$ (62,000)	\$ 1,447,759	\$ (2,370)	
Indirect Expenses	\$ 1,026,001	\$ 1,026,001	\$ -	\$ 998,750	\$ (27,251)	
Other Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	\$ -	
Total Expenses (B)	\$ 2,476,130	\$ 2,414,130	\$ (62,000)	\$ 2,446,509	\$ (29,621)	
Change in Net Assets (=A-B)	\$ 29,747	\$ 91,747	\$ 62,000	\$ 15,701	\$ (14,047)	
Total Funding (A) Requirement	\$ 2,446,383	\$ 2,446,383	\$ (62,000)	\$ 2,430,809	\$ (15,574)	
Fixed Asset Additions, excluding Right of Use Assets (C)	29,747	29,747	-	15,701	(14,047)	
TOTAL BUDGET (=B+C)	2,505,877	2,443,877	(62,000)	2,462,210	(43,668)	
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ 0	\$ 62,000	\$ 62,000	\$ (0)	\$ (0)	

Administrative Services

Administrative Services Program Resources						
(in whole dollars)						
	Direct Expenses			FTEs		
	2020 Budget	2021 Budget	Increase (Decrease)	2020 Budget	2021 Budget	Increase (Decrease)
Technical Committees and Members Forum	\$75,793	\$72,577	(\$3,215)	0.50	0.50	0.00
General and Administrative ²	\$3,874,453	\$3,973,516	\$99,063	2.73	3.23	0.50
Legal and Regulatory	\$761,007	\$756,124	(\$4,884)	2.00	2.00	0.00
Information Technology	\$1,144,119	\$1,340,544	\$196,424	2.00	2.55	0.55
Human Resources	\$158,731	\$67,666	(\$91,066)	1.00	0.50	-0.50
Finance and Accounting	\$703,291	\$736,448	\$33,157	2.00	2.00	0.00
Total Administrative Services ¹	\$6,717,395	\$6,946,875	\$229,480	10.23	10.78	0.55

¹ NPCC's 2021 Administrative Services Direct Expenses and Fixed Assets total \$6,946,875 of which \$395,801 is allocated to NPCC's Criteria Services division, which is a non-statutory function. As a result of the allocation to the Criteria Services division, the Administrative Expenditures included in the 2021 statutory budget are \$6,551,074 which is an increase of \$243,129 from the 2020 budget of \$6,307,945.

² Succession implementation costs of \$477,520 included in General and Administrative Direct Expenses will be funded from Board approved Business Continuity Reserves and will not impact assessments.

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.

Administrative Services

Funding sources and related expenses for the Administrative Services section of the 2021 business plan are shown in the table below. Explanations of variances by expense category are included within the Supplemental Tables found in Section B.

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
ADMINISTRATIVE SERVICES						
	2020 Budget	2020 Projection	Variance 2020 Projection v 2020 Budget Over(Under)	2021 Budget	Variance 2021 Budget v 2020 Budget Over(Under)	
Funding						
ERO Funding						
ERO Assessments	\$ (625,856)	\$ (625,856)	\$ -	\$ (148,158)	\$ 477,698	
Penalty Sanctions	-	-	-	-	-	
Total ERO Funding	\$ (625,856)	\$ (625,856)	\$ -	\$ (148,158)	\$ 477,698	
Membership Dues	-	-	-	-	-	
Testing Fees	-	-	-	-	-	
Services & Software	-	-	-	-	-	
Workshops & Misc Revenue	-	-	-	-	-	
Interest & Investment Income	55,800	55,800	-	56,275	475	
Total Funding (A)	\$ (570,056)	\$ (570,056)	\$ -	\$ (91,883)	\$ 478,173	
Expenses						
Personnel Expenses						
Salaries	\$ 2,433,049	\$ 2,433,049	\$ -	\$ 2,704,045	\$ 270,997	
Payroll Taxes	126,595	126,595	-	129,878	3,283	
Benefits	674,649	674,649	-	562,392	(112,257)	
Retirement Costs	313,571	313,571	-	336,149	22,577	
Total Personnel Expenses	\$ 3,547,864	\$ 3,547,864	\$ -	\$ 3,732,464	\$ 184,600	
Meeting Expenses						
Meetings & Conference Calls	\$ 162,750	\$ 162,750	\$ -	\$ 149,000	\$ (13,750)	
Travel	129,100	129,100	-	148,200	19,100	
Total Meeting Expenses	\$ 291,850	\$ 291,850	\$ -	\$ 297,200	\$ 5,350	
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ 361,000	\$ 361,000	\$ -	\$ 85,650	\$ (275,350)	
Office Rent	832,700	832,700	-	870,141	37,441	
Office Costs	685,981	685,981	-	811,420	125,439	
Professional Services	947,000	947,000	-	1,005,000	58,000	
Computer & Equipment Leases	-	-	-	-	-	
Miscellaneous	51,000	51,000	-	51,000	-	
Total Operating Expenses, excluding Depreciation	\$ 2,877,681	\$ 2,877,681	\$ -	\$ 2,823,211	\$ (54,470)	
Total Direct Expenses	\$ 6,717,395	\$ 6,717,395	\$ -	\$ 6,852,875	\$ 135,480	
Indirect Expenses	\$ (6,272,855)	\$ (6,272,855)	\$ -	\$ (6,375,355)	\$ (102,500)	
Other Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	\$ -	
Total Expenses (B)	\$ 444,540	\$ 444,540	\$ -	\$ 477,520	\$ 32,980	
Change in Net Assets (=A-B)	\$ (1,014,596)	\$ (1,014,596)	\$ -	\$ (569,403)	\$ 445,193	
Fixed Asset Additions, excluding Right of Use Assets (C)	\$ -	\$ -	\$ -	\$ -	\$ -	
TOTAL BUDGET (=B+C)	\$ 444,540	\$ 444,540	\$ -	\$ 477,520	\$ 32,980	
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ (1,014,596)	\$ (1,014,596)	\$ -	\$ (569,403)	\$ 445,193	

Technical Committees and Member Forums

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 subject matter 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.

2021 Key Assumptions

- NPCC's standing committee and subgroup structure for effective stakeholder involvement will continue in 2021.
- 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 2021.
- NPCC will continue to invest in technology and innovation to allow efficient collaboration on technical issues related to reliability.

Technical Committees and Member Forums 2021 Goals and Deliverables

- The 2021 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; and,
- 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 include, but are not limited to:
 - Conducting the Media Event – release of the Summer 2021 NPCC Reliability Assessment; and,
 - Participation in ERO Regional Communication Group 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.)

Resource Requirements

- No significant changes.

General and Administrative

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.

Resource Requirements

- During 2020 an executive search will be conducted in order to identify a successor CEO to transition into that role by vote of the Membership at its Annual Meeting in early December to become effective January 1, 2021. The incumbent President and CEO has identified a planned retirement at the end of first quarter of 2021. The expectation is that the identified successor will be retained effective January 1, 2021 coincident with the assumption of the Chief Executive Office. Costs related to the executive search recruiting efforts and succession plan implementation will be funded from the existing Business Continuity Reserve, identified by the NPCC Board of Directors in 2017 for release during 2020 and within 2021, as approved by the Board. Therefore, 2021 assessments will not be impacted by these President and CEO succession-related expenses.

Legal and Regulatory

Program Scope and Functional Description

NPCC's professional legal services provide counsel to the President and CEO, Board of Directors, Senior Vice President and COO, Treasurer, General Counsel and Secretary and staff on a wide range of legal, compliance and regulatory matters including legislation, corporate law, code of conduct, member services, privacy, confidentiality, governance, employment law, tax matters, contracts and other areas affecting NPCC. To ensure and maintain independence and objectivity consistent with ERO Enterprise value drivers, NPCC's in-house professional services evaluate internal controls and corporate, operational, strategic and reputational risk, and participate in risk identification, evaluation and mitigation activities. In-house professional legal services provide advice and advance significant corporate policy and strategic planning initiatives, assisting in the development of NPCC's strategic focus areas and their alignment with ERO Enterprise approaches. In addition, in-house professional legal services provide support to other program areas on matters arising in connection with the performance of NPCC's delegated functions to achieve organizational excellence consistent with NPCC's values. The Legal and Regulatory program area is also responsible for activities associated with the Corporate Secretary function such as preparing Board materials and minutes, facilitating and conducting Board training, and ensuring that meetings of the Board of Directors and Committees adhere to the Bylaws and other relevant governing documents. Outside counsel, as necessary, reviews complex matters for legal sufficiency and provides independent legal advice and guidance on certain employment and Human Resource related matters.

Resource Requirements

- No significant changes.

Information Technology

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 and all applicable Critical Electric Infrastructure Information protection and Confidentiality requirements. NPCC maintains an offsite backup server for continuity of essential operations in the event that its primary location is unavailable.

NPCC supports the ERO efforts to implement, operate and maintain software tools supporting common enterprise wide operations and leveraging ERO solutions which have been approved by the ERO Executive Committee (ERO EC), which is comprised of the senior leadership of NERC and each of the Regional Entities. NPCC's budget assumes the availability of enterprise software tools as described in NERC's business plan and budget. If implementation of these software applications is delayed or otherwise not available as planned, NPCC could incur additional costs to implement ERO Enterprise-wide programs pending the availability of these applications.

NERC and the Regional Entities are committed to working collaboratively to minimize duplication of effort and investments, and improve operational efficiency. This collaboration continues to refine existing strategies, governance and procurement practices applicable to the development, operation and maintenance of enterprise architecture, software and data systems supporting complementary and combined NERC and Regional Entity operations.

The NERC information technology budget does not supplant NPCC's need for IT expenditures for specific regional projects and internal region specific IT support needs. NPCC's 2021 Business Plan and Budget assumes agreed upon ERO Enterprise applications will be available and includes only NPCC costs for Region specific support needs.

2021 Key Assumptions

- Continue to maintain the compliance portal through collaboration with other Regional Entities and NERC (CUG), while transitioning to the ERO Enterprise CMEP data application (Align).
- Support the Event Analysis program through continued participation in the tools used for the tracking and analysis of system events and identification of better practice elements.
- Support the Bulk Electric System Exception Process (BEP) to enable and facilitate tracking and processing of exceptions submitted. 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.

2021 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:

- Implementation of a security control framework.
- Work with the ERO Enterprise to collaborate and implement a data loss prevention program.
- Continue to expand the utilization of the document management system throughout the company.

- Constantly review and evaluate security measures taken to reduce breach of security risks.
- Ensure all information systems are functional and secure, and that all applications running on those systems meet business requirements for performance, availability, and security.
- Provide outreach and education to NPCC members in IT best practices.
- Continually improve Disaster Recovery and Business Continuity policies and practices to ensure continuity and reliability of IT and business related services.
- Upgrade various hardware and equipment.

Resource Requirements

Personnel

- NPCC anticipates no need to hire additional personnel in this program area in 2021.

Fixed Assets

- Capital expenditures planned for 2021 include the implementation of a security controls framework and data loss prevention strategy, as well as continuing enhancement of the document management system and equipment upgrades.

Human Resources

Program Scope and Functional Description

NPCC has assembled an exceptional team of highly qualified employees to carry out its activities. 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; knowledge transfer, training and development; and employee time tracking.

Resource Requirements

- No significant changes.

Accounting and Finance

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 consistently identified this system as a best practice.

2021 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
- Alignment of changes in budget and changes in aggregate assessment
- 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 Variance Reports
- IRS Reporting
- Annual Independent Audit initiated by the Regional Entity

Resource Requirements

- No significant changes.

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 2019 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 2019 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 ISOs/BAAs within NPCC as the designees for the load serving entities (LSEs) in New York, New England, Ontario, Québec, New Brunswick and Nova Scotia.

In order to reflect and respect the international membership and nature of NPCC, any sub-Regional reliability assessment costs in response to U.S. only regulatory initiatives will be considered for allocation to U.S. only ISOs/BAAs consistent with NERC Rules of Procedure section 1102. Additionally, the compliance responsibilities and authorities within the U.S., and the specific compliance responsibilities within each of the Canadian provinces within NPCC, and 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 net energy for load (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 U.S. only reliability assessment and 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. In order to establish the RE division funding requirements for each Balancing Authority Area on a NEL basis for all programs except for Compliance, the proposed expenses and fixed assets of all other programs are calculated and the adjustment for the RE division cash reserve requirement is identified. 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. 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, with the resultant addition being the RE division assessment, without the compliance program costs, calculated on a NEL basis.

In accordance with the *NPCC Amended and Restated Bylaws* the CS division proposed expenses and fixed assets of all programs are calculated and the adjustment for the CS division cash reserve requirement is identified, with the resultant addition being the CS division funding requirement and assessment, calculated on a NEL basis.

For costs associated with the RE division compliance program, NPCC's allocation methodology apportions XX% of the costs for the program, attributed to CORC Fundamentals (CF), between the BAAs in the United States and Canada on a NEL basis.

Audits and Investigations (AI) related costs, representing XX% 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. 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.

The remaining XX% 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. Based on historical data, NPCC reviewed each BAAs percentage of violations, mitigation plans and settlement agreements to determine each BAA's total average percentage of enforcement activities. The portion allocated to the U.S. BAA's 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.

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.

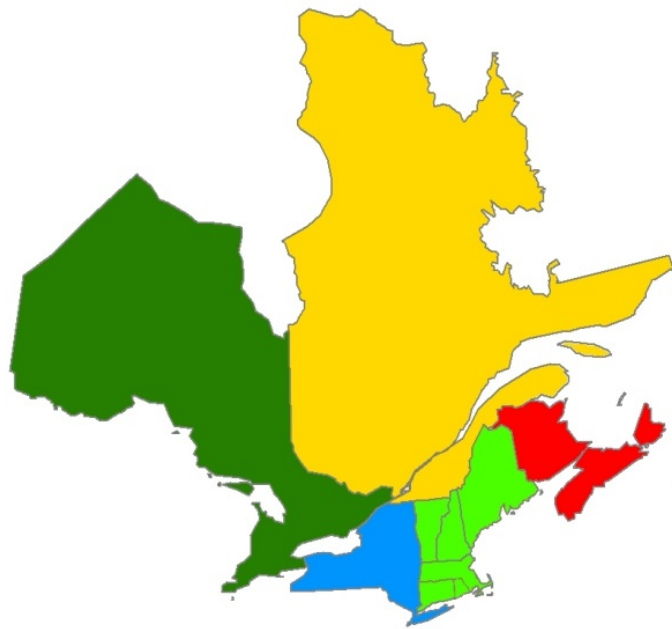
The CORC actual vs budget variance from the most recent year for which audited financials are available is broken out from the rest of the Adjustment to Cash Reserve and assigned to the CORC program allocation of costs. Within Québec these costs are funded directly by the regulator, therefore, the assignment of program area variances needs to respect those specific circumstances.

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.

		Table to be Inserted		

Section B — Supplemental Financial Information

2021 Business Plan and Budget



Section B – Supplemental Financial Information

Reserve Balance

Table B-1 Reserve Balance

Working Capital and Operating Reserve Analysis 2020-2021				
REGIONAL ENTITY DIVISION				
	Total Reserve	Operating Reserve	Working Capital	Business Continuity
Beginning Total Reserve, December 31, 2019	5,629,637	3,306,222	1,383,415	940,000
Plus: 2020 ERO Funding (from LSEs or designees)	15,338,737	15,338,737		
Plus: 2020 Other funding sources	89,550	89,550		
Less: 2020 Projected expenses & capital expenditures	(16,287,647)	(15,843,107)		(444,540)
Projected Total Reserve, December 31, 2020	4,770,276	2,891,401	1,383,415	495,460
Desired Total Reserve, December 31, 2021	4,195,858	2,781,386 ¹	1,396,533 ²	17,940 ³
Less: Projected Total Reserve, December 31, 2020	(4,770,276)	(2,891,401)	(1,383,415)	(495,460)
Increase(decrease) in assessments to achieve desired Total Reserve	(574,418)	(110,015)	13,117	(477,520)
2021 Expenses and Capital Expenditures	16,759,063			
Less: Penalty Sanctions ⁴	(604,000)			
Less: Other Funding Sources	(123,775)			
Less: Release of Business Continuity Reserve Funds ³	(477,520)			
Adjustment to Working Capital to achieve desired Total Reserve balance ²	13,117			
Adjustment to Operating Reserve to achieve desired Total Reserve balance ¹	(110,015)			
2021 Assessment	15,456,871			

¹ Operating Reserve within a range from 8.33% to 25.00% of Budget. \$2,781,386 represents 16.60% of the 2021 budget of \$16,759,063

² Working Capital equal to 8.33% of Budget. \$1,396,533 represents 8.33% of the 2021 budget of \$16,759,063

³ Business Continuity Reserve (BCR) established in 2017 as approved by the NPCC Board of Directors to fund Succession Planning related expenses.

⁴ Represents collections July 1, 2019 to June 30, 2020.

Explanation of Changes in Reserve Policy from Prior Year

There was no change to the existing Working Capital and Operating Reserve Policy. A separate Business Continuity Reserve (BCR) in the amount of \$1,000,000 (allocated between the Regional Entity and Criteria Services divisions) was established in 2017 as approved by the NPCC Board of Directors, upon recommendation by the Management Development and Compensation Committee and endorsement by the Finance and Audit Committee, to be drawn upon as subsequently brought before the Board of Directors for approval of release of funds in association with President & CEO succession related activities associated with the planned or a sudden retirement, as well as other sudden changing workforce staffing requirements which could be brought about by coincident multiple staff retirements.

Breakdown by Statement of Activity Sections

The following detailed schedules are in support of the Regional Entity division Statement of Activities on page 14 of the 2021 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, 2020 are to be used to offset assessments in the 2020 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, 2019 through June 30, 2020 are listed below. Penalty monies received from July 1, 2020 through June 30, 2021 will be used to offset U.S. load serving entity designee assessments in the 2022 Budget.

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, 2020	Date Received	Amount Received
	9/16/2019	\$ 50,000.00
	9/10/2019	\$ 20,000.00
	12/24/2019	\$ 84,000.00
	1/17/2020	\$ 450,000.00
Total Penalties Received		\$ 604,000.00

Table B-3 Supplemental Funding

Outside Funding Breakdown By Program (excluding ERO Assessments & Penalty Sanctions)	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget
Reliability Standards				
Total	\$ -	\$ -	\$ -	\$ -
Compliance Monitoring, Enforcement & Org. Registration				
	\$ -	\$ -	\$ -	\$ -
	-	-	-	-
Total	\$ -	\$ -	\$ -	\$ -
Reliability Assessment and Performance Analysis				
	\$ -	\$ -	\$ -	\$ -
	-	-	-	-
Total	\$ -	\$ -	\$ -	\$ -
Training and Education				
Workshops	\$ 67,500	\$ (33,750)	\$ 67,500	\$ -
Total	\$ 67,500	\$ (33,750)	\$ 67,500	\$ -
Situation Awareness and Infrastructure Security				
	\$ -	\$ -	\$ -	\$ -
Total	\$ -	\$ -	\$ -	\$ -
Technical Committees and Member Forums				
	\$ -	\$ -	\$ -	\$ -
Total	\$ -	\$ -	\$ -	\$ -
Administrative Services Programs				
Interest & Investment Income	\$ 55,800	\$ 55,800	\$ 56,275	\$ 475
Total	\$ 55,800	\$ 55,800	\$ 56,275	\$ 475
Total Outside Funding	\$ 123,300	\$ 22,050	\$ 123,775	\$ 475

Explanation of Significant Variances

- NPCC Spring Workshop was held via webinar due to the COVID-19 pandemic. NPCC plans to hold two in-person workshops in 2021.
- NPCC estimates interest & investment income of \$56,328 in 2021 from investment of reserves in a 100% U.S. Treasury Securities money market fund, which will offset 2021 assessments.

Table B-4 Personnel Expenses

Personnel Expenses	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Salaries					
Salary	\$ 7,664,262	\$ 7,664,262	\$ 7,885,535	\$ 221,273	2.9%
Employment Agency Fees	\$ 16,000	\$ 16,000	\$ 170,000	\$ 154,000	962.5%
Temporary Office Services	\$ 24,000	\$ 24,000	\$ 18,000	\$ (6,000)	-25.0%
Total Salaries	\$ 7,704,262	\$ 7,704,262	\$ 8,073,535	\$ 369,273	4.8%
Total Payroll Taxes	\$ 479,019	\$ 479,019	\$ 493,288	\$ 14,269	3.0%
Benefits					
Education Reimbursement	\$ 27,500	\$ 27,500	\$ 16,000	\$ (11,500)	-41.8%
Training and Seminars	\$ 83,580	\$ 83,580	\$ 82,494	\$ (1,086)	-1.3%
Medical Insurance	\$ 1,168,854	\$ 1,168,854	\$ 1,295,850	\$ 126,996	10.9%
Life-LTD-STD Insurance	\$ 110,889	\$ 110,889	\$ 110,466	\$ (423)	-0.4%
Worker's Compensation	\$ 32,000	\$ 32,000	\$ 27,400	\$ (4,600)	-14.4%
Vacation	\$ 504,062	\$ 504,062	\$ 503,237	\$ (825)	-0.2%
Relocation	\$ -	\$ -	\$ -	\$ -	-
Total Benefits	\$ 1,926,885	\$ 1,926,885	\$ 2,035,447	\$ 108,563	5.6%
Retirement					
Pension Contribution	\$ -	\$ -	\$ -	\$ -	-
Employee Savings Plan	\$ 770,950	\$ 770,950	\$ 808,033	\$ 37,083	4.8%
Savings Admin	\$ 36,000	\$ 36,000	\$ 36,000	\$ -	0.0%
Deferred Compensation	\$ 76,000	\$ 76,000	\$ 76,000	\$ -	0.0%
Total Retirement	\$ 882,950	\$ 882,950	\$ 920,033	\$ 37,083	4.2%
Total Personnel Costs	\$ 10,993,117	\$ 10,993,117	\$ 11,522,303	\$ 529,187	4.8%
FTEs	41.09	41.09	43.11	2.02	4.9%
Cost per FTE					
Salaries	\$ 187,497	\$ 187,497	\$ 187,278	\$ (220)	-0.1%
Payroll Taxes	\$ 11,658	\$ 11,658	\$ 11,443	\$ (215)	-1.8%
Benefits	\$ 46,894	\$ 46,894	\$ 47,215	\$ 321	0.7%
Retirement	\$ 21,488	\$ 21,488	\$ 21,342	\$ (147)	-0.7%
Total Cost per FTE	\$ 267,538	\$ 267,538	\$ 267,277	\$ (261)	-0.1%

Explanation of Significant Variances

- Increase of two FTE's in 2021.
- Staff vacancy rate increased to 6% in 2021 from 0% in 2020.
- Increase in Employment Agency Fees represents recruiting fees to retain experienced engineers as a part of succession planning.
- Increase in Training and Seminars is due to an increase per employee training budget.
- Medical insurance increase reflects a premium increase of 10%. Additionally, fewer employees are waiving NPCC coverage for that of a prior employer.
- Personnel expenses include succession planning related costs that will be funded through business continuity reserves and do not impact assessments.

Table B-5 Meeting Expense

Meeting Expenses	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Meetings	\$ 361,750	\$ 361,750	\$ 372,000	\$ 10,250	2.8%
Travel	\$ 845,900	\$ 845,900	\$ 884,200	\$ 38,300	4.5%
Conference Calls	\$ 36,000	\$ 36,000	\$ 9,000	\$ (27,000)	-75.0%
Total Meeting Expenses	\$ 1,243,650	\$ 1,243,650	\$ 1,265,200	\$ 21,550	1.7%

Explanation of Significant Variances

- Decrease in conference calls expense is a result of ERO Enterprise contracted rate.

Table B-6 Consultants and Contracts

Consultants	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Consultants					
Reliability Standards	\$ -	\$ -	\$ -	\$ -	-
Compliance Enforcement and Organization Registration and Certification	\$ -	\$ -	\$ -	\$ -	-
Reliability Assessment and Performance Analysis	\$ -	\$ -	\$ -	\$ -	-
Training and Education	\$ -	\$ -	\$ -	\$ -	-
Situation Awareness and Infrastructure Security	\$ -	\$ -	\$ -	\$ -	-
Member Forums	\$ -	\$ -	\$ -	\$ -	-
General and Administrative	\$ 279,000	\$ 279,000	\$ -	\$ (279,000)	-100.0%
Legal and Regulatory	\$ -	\$ -	\$ -	\$ -	-
Information Technology	\$ -	\$ -	\$ -	\$ -	-
Human Resources	\$ -	\$ -	\$ -	\$ -	-
Accounting and Finance	\$ -	\$ -	\$ -	\$ -	-
Consultants Total	\$ 279,000	\$ 279,000	\$ -	\$ (279,000)	-100.0%
Contracts	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Reliability Standards	\$ 20,000	\$ 20,000	\$ 20,000	\$ -	0.0%
Compliance Enforcement and Organization Registration and Certification	\$ 1,097,150	\$ 1,097,150	\$ 707,150	\$ (390,000)	-35.5%
Reliability Assessment and Performance Analysis	\$ 533,000	\$ 533,000	\$ 647,000	\$ 114,000	21.4%
Training and Education	\$ -	\$ -	\$ -	\$ -	-
Situation Awareness and Infrastructure Security	\$ 60,000	\$ 60,000	\$ 50,000	\$ (10,000)	-16.7%
Member Forums	\$ -	\$ -	\$ -	\$ -	-
General and Administrative	\$ 75,000	\$ 75,000	\$ 80,000	\$ 5,000	6.7%
Legal and Regulatory	\$ -	\$ -	\$ -	\$ -	-
Information Technology	\$ -	\$ -	\$ -	\$ -	-
Human Resources	\$ -	\$ -	\$ -	\$ -	-
Accounting and Finance	\$ 7,000	\$ 7,000	\$ 5,650	\$ (1,350)	-19.3%
Contracts Total	\$ 1,792,150	\$ 1,792,150	\$ 1,509,800	\$ (282,350)	-15.8%
Total Consultants and Contracts	\$ 2,071,150	\$ 2,071,150	\$ 1,509,800	\$ (561,350)	-27.1%

Explanation of Significant Variances

- General and Administrative consulting costs in 2020 are related to an executive search to identify a successor CEO. The search is expected to be completed during 2020.
- Ongoing effort to decrease the use of consultants and contractors when possible. (See program area sections for detail regarding a specific program area.)

Table B-7 Office Rent

Office Rent	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Office Rent	\$ 650,000	\$ 650,000	\$ 650,000	\$ -	0.0%
Utilities	\$ 47,000	\$ 47,000	\$ 47,000	\$ -	0.0%
Maintenance	\$ 37,000	\$ 37,000	\$ 45,000	\$ 8,000	21.6%
Security	\$ 2,700	\$ 2,700	\$ 3,141	\$ 441	16.3%
Real Estate Taxes	\$ 96,000	\$ 96,000	\$ 125,000	\$ 29,000	30.2%
Total Office Rent	\$ 832,700	\$ 832,700	\$ 870,141	\$ 37,441	4.5%

Explanation of Significant Variances

- Increases in Maintenance and Real Estate Taxes are based on historical actual expenses.

Table B-8 Office Costs

Office Costs	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Telephone	\$ 88,720	\$ 88,720	\$ 88,720	\$ -	0.0%
Internet Expense	\$ 74,340	\$ 74,340	\$ 70,500	\$ (3,840)	-5.2%
Office Supplies	\$ 33,000	\$ 33,000	\$ 28,000	\$ (5,000)	-15.2%
Computer Supplies and Maintenance	\$ 424,921	\$ 424,921	\$ 576,000	\$ 151,079	35.6%
Subscriptions & Publications	\$ 14,000	\$ 14,000	\$ 20,000	\$ 6,000	42.9%
Dues	\$ 3,400	\$ 3,400	\$ 9,000	\$ 5,600	164.7%
Postage	\$ 1,200	\$ 1,200	\$ 1,200	\$ -	0.0%
Express Shipping	\$ 6,000	\$ 6,000	\$ 6,000	\$ -	0.0%
Copying	\$ 26,400	\$ 26,400	\$ 24,000	\$ (2,400)	-9.1%
Reports	\$ 2,000	\$ 2,000	\$ 2,000	\$ -	0.0%
Stationary and Office Forms	\$ 2,000	\$ 2,000	\$ 2,000	\$ -	0.0%
Equipment Repair/Service Contracts	\$ -	\$ -	\$ -	\$ -	-
Bank Charges	\$ 10,000	\$ 10,000	\$ 10,000	\$ -	0.0%
Sales and Use Tax	\$ -	\$ -	\$ -	\$ -	-
Merchant Credit Card Fees	\$ -	\$ -	\$ -	\$ -	-
Presentation and Publicity	\$ -	\$ -	\$ -	\$ -	-
Total Office Costs	\$ 685,981	\$ 685,981	\$ 837,420	\$ 151,439	22.1%

Explanation of Significant Variances

- Increase in Computer Supplies and Maintenance is related to various security and network infrastructure improvements. (See Information Technology program area section for additional details.)

Table B-9 Professional Services

Professional Services	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
BOT Fee	\$ 332,000	\$ 332,000	\$ 300,000	\$ (32,000)	-9.6%
BOT Search Fee	\$ -	\$ -	\$ -	\$ -	-
Legal - Reorganization	\$ -	\$ -	\$ -	\$ -	-
Accounting & Auditing Fees	\$ 310,000	\$ 310,000	\$ 370,000	\$ 60,000	19.4%
Legal Fees - Other	\$ 235,000	\$ 235,000	\$ 260,000	\$ 25,000	10.6%
Insurance - Commercial	\$ 70,000	\$ 70,000	\$ 75,000	\$ 5,000	7.1%
Total Services	\$ 947,000	\$ 947,000	\$ 1,005,000	\$ 58,000	6.1%

Explanation of Significant Variances

- Consultant treasurer related fees were reclassified from BOT Fee to Accounting & Auditing Fees.

Table B-10 Miscellaneous

Miscellaneous Expense	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Miscellaneous Expense	\$ 51,000	\$ 51,000	\$ 51,000	\$ -	0.0%
Total Miscellaneous Expense	\$ 51,000	\$ 51,000	\$ 51,000	\$ -	0.0%

Table B-11 Other Non-Operating Expenses

Other Non-Operating Expenses	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Interest Expense	\$ -	\$ -	\$ -	\$ -	-
Office Relocation	\$ -	\$ -	\$ -	\$ -	-
Total Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	-

Table B-12 Fixed Assets

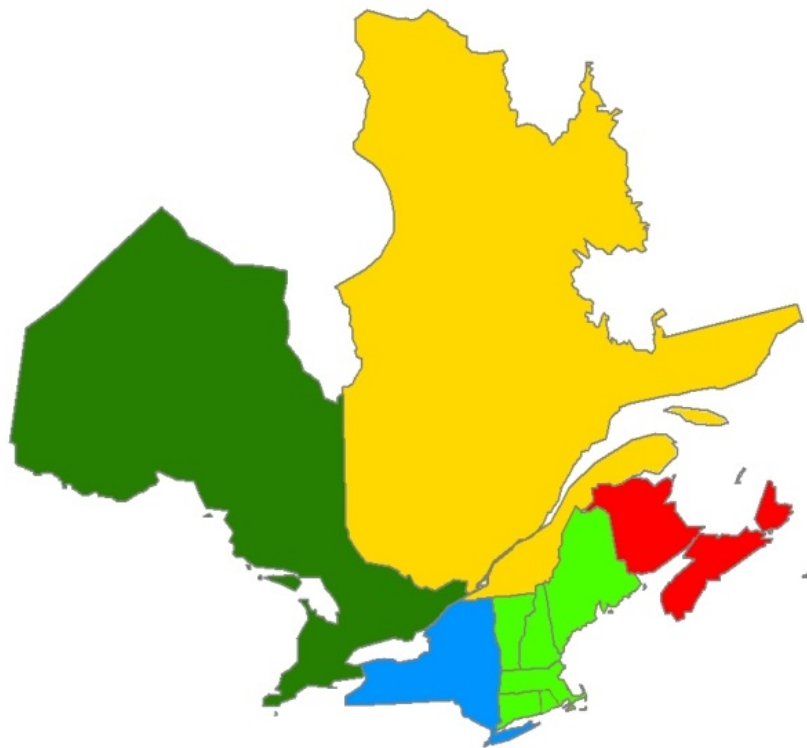
Fixed Asset Additions	Budget 2020	Projection 2020	Budget 2021	Variance 2021 Budget v 2020 Budget	Variance %
Equipment CapEx	\$ -	\$ -	\$ -	\$ -	-
Computer & Software CapEx	\$ 170,000	\$ 170,000	\$ 65,800	\$ (104,200)	-61.3%
Furniture & Fixtures CapEx	\$ -	\$ -	\$ 14,100	\$ 14,100	-
Leasehold Improvements	\$ -	\$ -	\$ 14,100	\$ 14,100	-
Allocation of Fixed Assets	\$ -	\$ -	\$ -	\$ -	-
Total Fixed Asset Additions	\$ 170,000	\$ 170,000	\$ 94,000	\$ (76,000)	-44.7%

Explanation of Significant Variances

- Computer and software capital expenditures include the implementation of a security controls framework and data loss prevention strategy, as well as continuing enhancement of the document management system and equipment upgrades.
- Other planned capital expenditures include reconfigurations of office space related to succession planning.

Table B-13

Section C — Criteria Services Division Activities 2021 Business Plan and Budget



Section C – Criteria Services Division Activities

Criteria Services Division (in whole dollars)			
	2020 Budget	2021 Budget	Increase (Decrease)
Total FTEs	2.14	2.14	0.00
Total Direct Expenses	\$662,756	\$619,451	(\$43,305)
Total Indirect Expenses	\$415,818	\$395,801	(\$20,017)
Other Non-Operating Expenses	\$0	\$0	\$0
Working Capital and Operating Reserves Requirement	(\$49,707)	(\$311,055)	(\$261,347)
Fixed Asset Additions	\$30,000	\$6,000	(\$24,000)
Funding Requirement	\$1,058,866	\$710,197	(\$348,670)

NPCC Regionally-Specific Criteria Services Background

NPCC Criteria Services division activities are based on the development, maintenance (including retirement when no longer needed), and promulgation of new or revised Regionally-specific, more stringent reliability criteria and supporting guideline or procedural documents. The requirements in NPCC Reliability Criteria apply only to those facilities defined as NPCC Bulk Power System elements through the performance based methodology identified in the NPCC Document A-10, “Classification of Bulk Power System Elements.”

In accordance with the NERC Rules of Procedure (RoP) Section 313, Regional Entities may develop Regional Criteria necessary to implement, augment, or facilitate compliance with NERC Reliability Standards. NPCC’s Directories contain Regional Criteria which consists of requirements which provide an increased level of reliability to the NPCC defined bulk power system. The criteria impose more stringent requirements than those which appear in the NERC reliability standards. The Regional Criteria may also be utilized to address issues not within the scope or jurisdiction of FERC as outlined in Section 215 of the Federal Power Act, such as resource adequacy. Regional Criteria may also address Canadian Provincial reliability issues, and may include specific operating or planning parameters, guides, agreements, protocols or other documents used to enhance the reliability of the Bulk Power System in the Region. These documents typically provide benefits by promoting more consistent implementation of the NERC Reliability Standards within the Region. These documents are not NERC Reliability Standards, Regional Reliability Standards, or Regional Variances, and therefore are not enforceable under the authority delegated by NERC pursuant to delegation agreements.

On a periodic basis and also as NERC Reliability Standards are revised or new standards are developed, NPCC performs reviews of any associated Regional Criteria for possible impact (e.g. continued need or revision). During the criteria review process NPCC’s Task Forces review not only the incremental reliability benefit, but also the cost effectiveness of the criteria. In addition, as NERC standards are improved, revised, and ultimately approved by the FERC some requirements of the NPCC Regional Criteria may become unnecessary in the US portion of NPCC. In these situations it is important that the criteria remains in place until such time as the all NPCC’s Canadian Provincial regulators adopt the NERC standard to ensure no reliability gaps exist.

For 2021 and beyond, the potential reliability impacts of increased penetration of Distributed Energy Resources (DER, e.g. solar and wind), and changing fuel mixes warrant further

consideration. The Criteria Services Division has a unique opportunity to review these issues and develop criteria, guideline, and procedural documents for DER which may be outside of the jurisdiction of FERC and NERC Reliability Standards. Participation of the entities responsible for development of DER renewable resources to develop reliability documents will become increasingly important over time. Outreach, collaboration, and coordination of topics related to DER will enable NPCC to develop guidance allowing more effective integration of these resources.

Increasing resilience of the BPS through alternative approaches to standards development using potential NPCC criteria, guidelines, and whitepapers will also be continually reviewed by NPCC's body of subject matter experts.

Membership and Governance

Full members, in accordance with NPCC's Amended and Restated Bylaws, are subject to compliance with Regionally-specific criteria 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.

Under Criteria Services NPCC will identify for membership, those entities involved in emerging technologies to assure that those entities that have an impact on Bulk Electric System reliability are included in appropriate NPCC activities.

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.

2021 Assumptions and Cost Impacts

The Criteria Services division activities are expected to remain stable or slightly increase throughout 2020 depending on reliability need.

- The Criteria Compliance Enforcement Program (CCEP) review and evaluation process is the mechanism for monitoring key criteria attributes as determined by the respective NPCC Task Forces and the Compliance Committee.
- Past non-compliances, if any, followed the due process stated in the CCEP-1 process document and proper resolution/enforcement action taken.

2021 Primary Goals and Objectives

- Continue with the development and maintenance of a set of NPCC Directories which augment or add specificity to the NERC Reliability Standards and which clearly delineate the more stringent NPCC criteria requirements. The combination of North American and more stringent NPCC Regional criteria provide for consistency and operational clarity while providing more robust defense in-depth, results based, criteria requirements to ensure NPCC BPS reliability.
- Continually review the criteria found in the NPCC Directories and the ERO standards to ensure no redundancies or inconsistencies exist.
- Retire Directories and/or Criteria which have been overtaken by improved NERC standards.
 - Directory No. 12 “Automatic Underfrequency Load Shedding Requirements” will be retired in 2021 upon approval of PRC-006-NPCC-2 “Automatic Underfrequency Load Shedding” Regional Standard by all the Canadian Provincial Authorities
- Identify opportunities to develop criteria, procedures or guideline documents to address reliability related matters with DER.
- Identify opportunities to address improvements in BES resilience with NPCC processes and documentation.
- Continually review the need to file revised and updated more stringent requirements with the New York State Department of Public Service and Canadian Provinces as applicable.
- Review, maintain, and revise the NPCC Regional Reliability Directories to facilitate compliance assessments and ensure the Criteria portions of the Directories augment and are not 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 any 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.
- Continually review impact of Bulk Electric System definition on Directory and Criteria content and compliance reporting.
- Continually review potential impacts of Sector or NPCC organizational changes on the Directories and Criteria by performing a review of enforcement and arbitration processes as needed.
- 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 clarifications for NPCC Criteria with the necessary subject matter experts and also identify any other 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 augment, add specificity, or address issues not covered in the NERC Reliability Standards as mandated by the NERC Rules of Procedure. The conversion of NPCC’s reliability criteria into Directories was undertaken to remove any redundancies with the NERC or NPCC Regional Reliability Standards and to clearly delineate the more stringent NPCC criteria requirements, assign Functional Model designations to those responsible for compliance and create measurable compliance criteria. Subsequent to the initial establishment of the Directories, which also organized functionally related B Guidelines and C Procedures into a single Directory, the

Directories were further reviewed to translate existing criteria language into a requirements and “standards type” format. The development of the criteria into NERC style requirements facilitates the NPCC Region’s CCEP and also ensures the delineation of the more stringent and more specific Regional criteria from the latest approved and effective set of NERC ERO standards.

In 2021, work will continue with the maintenance, revision, or potential retirement of individual Directories to address any actual or anticipated redundancies with new or modified NERC or NPCC Reliability Standards. The ongoing review and maintenance of the Directories will require Task Force and Criteria Services staff to support this effort and to serve as subject matter experts. In addition to the ongoing review of the criteria within the Directories for potential duplicity with the NERC standards, any Directories that have not had the criteria translated into NERC style requirements will also be reviewed in order to achieve criteria “requirements” which are clear, concise and measurable. Also, a standards style template will continue to be applied to the existing Directories to make them more consistent with the format of NERC standards. As NERC standards improve, the need for NPCC Directories and the amount of criteria contained therein may decrease over time, however in the interim, significant review is necessary to ensure the criteria remain consistent with the NERC standards as outlined in the NERC Rules of Procedure. NPCC will conduct internal reviews of all draft standards against Regional criteria and utilize subject matter experts to identify reliability and compliance related concerns. NPCC will file the revised NPCC Directories and notifications of retirements of Directories with the Canadian governmental and/or provincial Regulatory authorities within the NPCC “footprint”, on an as needed basis, in accordance with established provincial procedures and agreements executed with NPCC.

Additionally, as NERC Reliability Standards are developed, associated Directories will be reviewed for continued need. This review will identify the incremental reliability enhancement the Directory’s criteria will yield, determine if the enhancement is sufficient to warrant retention and if so, are there any potential cost effective alternatives that may exist to achieve that enhanced level of reliability.

NPCC Operations and Planning Directories

The following Directories are envisioned to remain active for 2021.

Directory #1, Design and Operation of the Bulk Power System.

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 TFCP and TFCO completed a review of the Directory#1 criteria in 2019, during which the criteria was translated into NERC style requirements and revisions were enacted to ensure consistency with recent changes to the TPL and TOP standards.

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 is reviewed this Directory in 2019.

Directory #4, System Protection Criteria

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 next review and revision.

Directory #5, *Reserve*

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 and ensure consistency with the BAL standards under revision in 2020.

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 reviewed and revised the document in 2020 to ensure consistency with the Remedial Action Scheme PRC-012 standard.

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 the review and revision of this Directory in 2021.

Directory #11, *Disturbance Monitoring Equipment*,

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 developed Directory#11 in order to facilitate the retirement of the NPCC Regional Standard PRC -002-NPCC-1.

NPCC Criteria Compliance and Enforcement Program (CCEP)

The NPCC Criteria Services division supports the reliable operation of the NPCC Bulk Power System (BPS) through implementation of the NPCC Criteria Compliance Program (CCEP). This program monitors, assesses, and enforces compliance on a subset of the regionally specific, more stringent NPCC Criteria that are unique to the NPCC BPS and are not duplicative of the NERC Reliability Standards. The physical characteristics and topology of the transmission system within the Region require that certain aspects of criteria be monitored for compliance.

The Criteria Services division and the NPCC Compliance Committee (CC) administer the CCEP. The CC is a stakeholder body consisting of NPCC Members and is structured by the seven sectors that appear in the NPCC Bylaws.

Noncompliance to NPCC Criteria is not subject to monetary sanctions and results in a notification of noncompliance to the Chief Executive Officer of the appropriate Full Member.

The CCEP program is described in document CCEP-1, *NPCC Criteria Compliance and Enforcement Program (CCEP) Process Document*. The CC reviews CCEP-1 annually and revisions to CCEP-1 are reviewed and approved by the CC.

The CCEP-1 document:

1. Provides a comprehensive CCEP Process Flow Diagram showing the process of evaluating and approving Criteria Certification submittals, and additional processes and responsibilities in the event that noncompliances, disputes, and sanctions arise;

2. Describes the roles and responsibilities of Reporting Members, the CC, the NPCC Reliability Coordinating Committee, and the Enforcement Panel in the compliance review and enforcement process
3. Describes non-monetary Sanctions, the Lateness Policy, and the Arbitration/Dispute Resolution process
4. Addresses the development of Mitigation Plans for any violations under the enforcement process

The CCEP Working Group (under the CC) develops a draft of the annual CCEP Implementation Plan and updates the blank certification templates for the upcoming Plan year. The Implementation Plan identifies the subset of Criteria that must be certified to and includes the certification form due dates. The draft CCEP Implementation Plan for the coming year and the draft certification templates are then submitted to the CC for review and approval.

The CC members review the completed certification forms that are returned by Full Members. NPCC staff develops an assessment report and scorecard that summarizes the certifications that were received for the CC to review and approve. The assessment report and any recommendations on non-compliances are then presented to the NPCC Reliability Coordinating Committee (RCC) for approval.

Compliance to the NPCC Criteria is a responsibility of the NPCC Members and is codified in the *AMENDED AND RESTATED BYLAWS OF NORTHEAST POWER COORDINATING COUNCIL, INC.* Implementation of the CCEP is also consist with the current Memorandum of Understanding that NPCC has with its Canadian Members.

Resource Requirements

- No significant changes.

2020 Budget and Projection and 2021 Budget Comparisons

Statement of Activities and Capital Expenditures 2020 Budget & Projection, and 2021 Budget						
CRITERIA SERVICES DIVISION						
	2020 Budget	2020 Projection	Variance 2020 Projection v 2020 Budget Over(Under)	2021 Budget	Variance 2021 Budget v 2020 Budget Over(Under)	
Funding						
ERO Funding						
ERO Assessments	\$ -	\$ -	\$ -	\$ -	\$ -	
Penalty Sanctions	-	-	-	-	-	
Total ERO Funding	\$ -	\$ -	\$ -	\$ -	\$ -	
Membership Dues	1,065,202	1,065,202	-	706,472	(358,730)	
Testing Fees	-	-	-	-	-	
Services & Software	-	-	-	-	-	
Workshops & Misc Revenue	-	-	-	-	-	
Interest & Investment Income	4,200	4,200	-	3,725	(475)	
Total Funding (A)	\$ 1,069,402	\$ 1,069,402	\$ -	\$ 710,197	\$ (359,205)	
Expenses						
Personnel Expenses						
Salaries	\$ 367,979	\$ 367,979	\$ -	\$ 336,972	\$ (31,008)	
Payroll Taxes	24,864	24,864	-	23,390	(1,474)	
Benefits	123,261	123,261	-	86,435	(36,826)	
Retirement Costs	41,954	41,954	-	36,654	(5,299)	
Total Personnel Expenses	\$ 558,057	\$ 558,057	\$ -	\$ 483,451	\$ (74,607)	
Meeting Expenses						
Meetings	\$ 14,000	\$ 14,000	\$ -	\$ 13,500	\$ (500)	
Travel	56,800	56,800	-	56,800	-	
Total Meeting Expenses	\$ 70,800	\$ 70,800	\$ -	\$ 70,300	\$ (500)	
Operating Expenses, excluding Depreciation						
Consultants & Contracts	\$ 76,360	\$ 76,360	\$ -	\$ 57,700	\$ (18,660)	
Office Rent	-	-	-	-	-	
Office Costs	-	-	-	4,000	4,000	
Professional Services	-	-	-	-	-	
Computer & Equipment Leases	-	-	-	-	-	
Miscellaneous	4,000	4,000	-	4,000	-	
Total Operating Expenses, excluding Depreciation	\$ 80,360	\$ 80,360	\$ -	\$ 65,700	\$ (14,660)	
Total Direct Expenses	\$ 709,217	\$ 709,217	\$ -	\$ 619,451	\$ (89,767)	
Indirect Expenses	\$ 409,450	\$ 409,450	\$ -	\$ 395,801	\$ (13,649)	
Other Non-Operating Expenses	\$ -	\$ -	\$ -	\$ -	\$ -	
Total Expenses (B)	\$ 1,118,668	\$ 1,118,668	\$ -	\$ 1,015,252	\$ (103,416)	
Change in Net Assets (=A-B)	\$ (49,265)	\$ (49,265)	\$ -	\$ (305,055)	\$ (255,789)	
Fixed Asset Additions, excluding Right of Use Assets (C)	\$ 30,000	\$ 30,000	\$ -	\$ 6,000	\$ (24,000)	
TOTAL BUDGET (=B+C)	\$ 1,148,668	\$ 1,148,668	\$ -	\$ 1,021,252	\$ (127,416)	
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	\$ (79,265)	\$ (79,265)	\$ -	\$ (311,055)	\$ (231,789)	

Personnel Analysis

Total FTE's by Program Area	Budget 2020	Projection 2020	Direct FTEs 2021 Budget	Shared FTEs ¹ 2021 Budget	Total FTEs 2021 Budget	Change from 2020 Budget
CRITERIA SERVICES DIVISION						
Operational Programs						
Reliability Standards	1.08	1.08	1.00	0.07	1.07	-0.01
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	1.08	1.08	1.00	0.07	1.07	-0.01
Situation Awareness and Infrastructure Security	0.00	0.00	0.00	0.00	0.00	0.00
Total FTEs Operational Programs	2.16	2.16	2.00	0.14	2.14	-0.02
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	2.16	2.16	2.00	0.14	2.14	-0.02

¹A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

Reserve Analysis

Working Capital and Operating Reserve Analysis 2020-2021				
CRITERIA SERVICES DIVISION				
	Total Reserve	Operating Reserve	Working Capital	Business Continuity
Beginning Total Reserve, December 31, 2019	737,914	589,159	88,755	60,000
2020 Non-Statutory Funding (from members)	1,065,202	1,065,202		
Plus: 2020 Other funding sources	0	0		
Less: 2020 Projected expenses & fixed asset additions	(1,148,668)	(1,122,128)		(26,540)
Projected Total Reserve, December 31, 2020	654,449	532,234	88,755	33,460
 Desired Total Reserve, December 31, 2021	 343,394	 255,313 ¹	 85,101 ²	 2,980 ³
Less: Projected Total Reserve, December 31, 2020	(654,449)	(532,234)	(88,755)	(33,460)
Increase(decrease) in assessments to achieve desired Total Reserve	(311,055)	(276,921)	(3,654)	(30,480)
2021 Funding requirement for expenses and fixed asset additions	1,021,252			
Less: Other Funding Sources	(3,725)			
Less: Release of Business Continuity Reserve Funds ³	(30,480)			
Adjustment to Working Capital to achieve desired Total Reserve balance ²	(3,654)			
Adjustment to Operating Reserve to achieve desired Total Reserve balance ¹	(276,921)			
2021 Funding and reserve requirement	706,472			

¹ Operating Reserve must be within a range from 8.33% to 25.00% of Budget. \$255,313 represents 25.00% of the 2021 budget of \$1,021,252.

² Working Capital must equal 8.33% of Budget. \$85,101 represents 8.33% of the 2021 budget of \$1,021,252.

³ Business Continuity Reserve (BCR) established in 2017 as approved by the NPCC Board of Directors to fund Succession Planning related expenses.

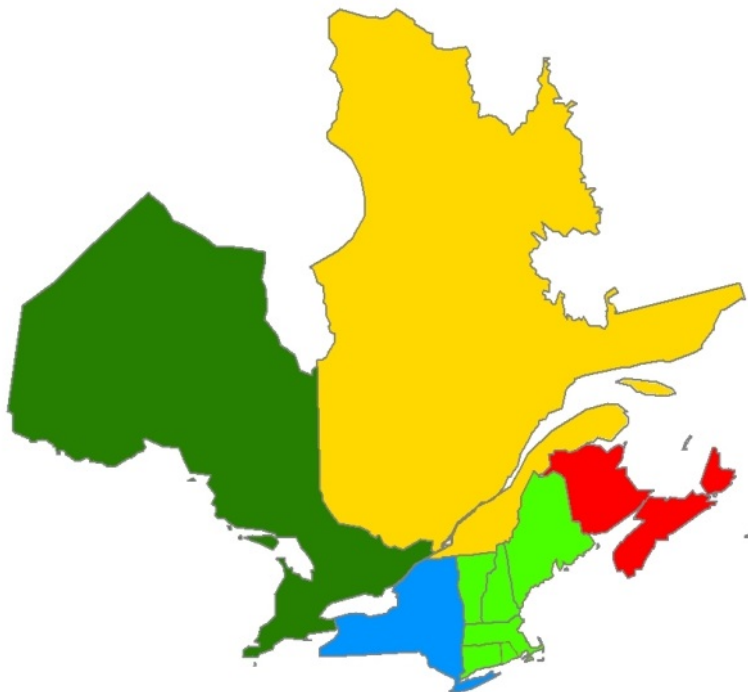
Explanation of Changes in Reserve Policy from Prior Year

There was no change to the existing Working Capital and Operating Reserve Policy. For 2021, Criteria Services assessments are decreasing by a percentage greater than decrease in budget in order to reduce the operating reserve in accordance with the established range. The Operating reserve must be within a range from 8.33% to 25.00% of budget. The projected operating reserve balance at year end 2021 of \$255,313 represents 25.00% of the 2021 Criteria Services budget of \$1,021,252.

A separate Business Continuity Reserve (BCR) in the amount of \$1,000,000 (allocated between the Regional Entity and Criteria Services divisions) was established in 2017 as approved by the NPCC Board of Directors, upon recommendation by the Management Development and Compensation Committee and endorsement by the Finance and Audit Committee, to be drawn upon as subsequently brought before the Board of Directors for approval of release of funds in association with President & CEO succession related activities associated with the planned or a sudden retirement, as well as other sudden changing workforce staffing requirements which could be brought about by coincident multiple staff retirements.

Section D – Additional Consolidated Financial Statements

2021 Business Plan and Budget



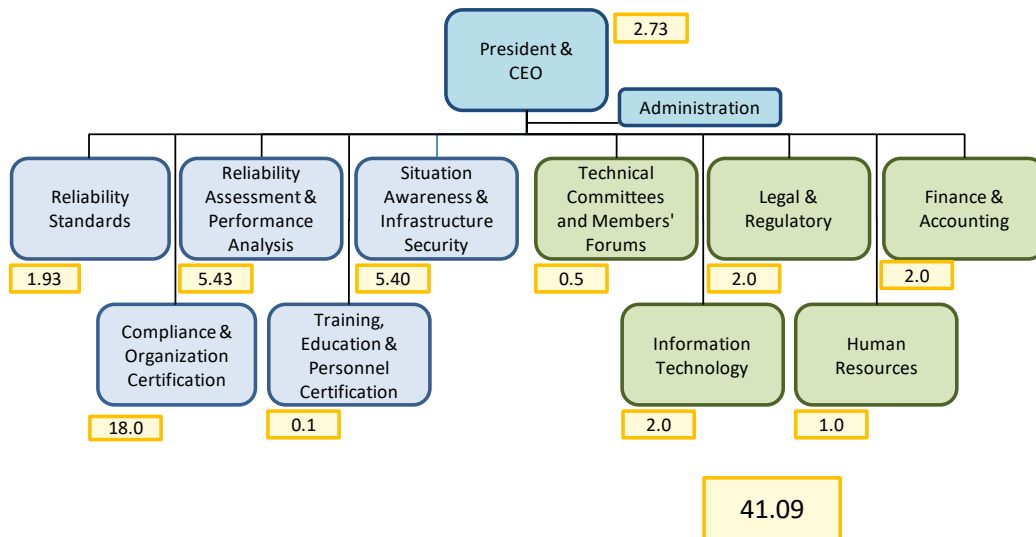
Section D — Additional Financial Statements

Statement of Financial Position

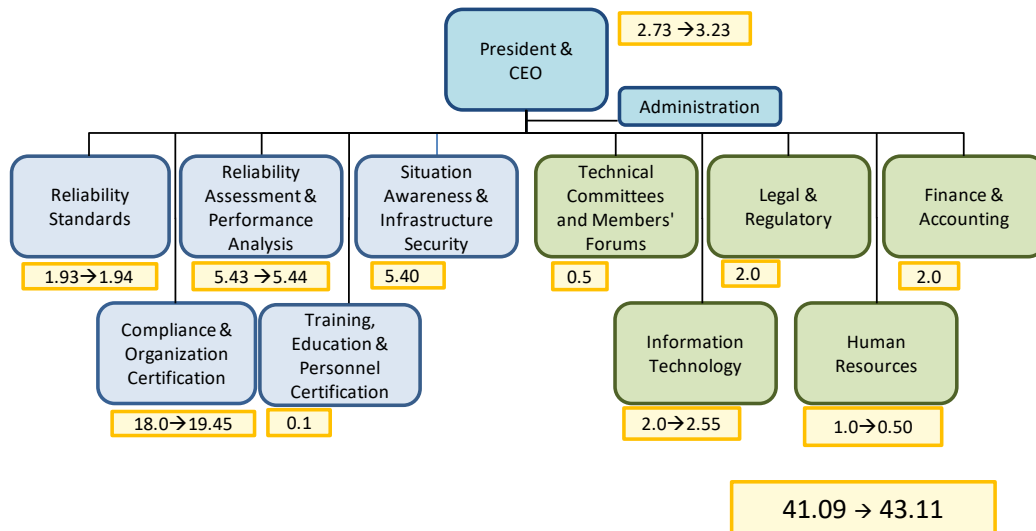
		Table to be Inserted		

Appendix A Staff Allocations

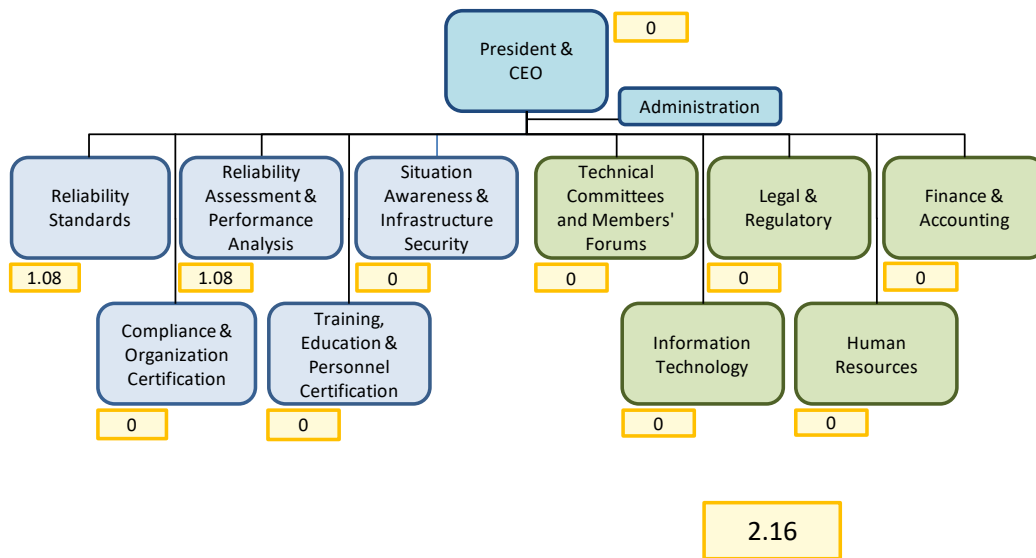
2020 Budget Staff Allocations - RE Division



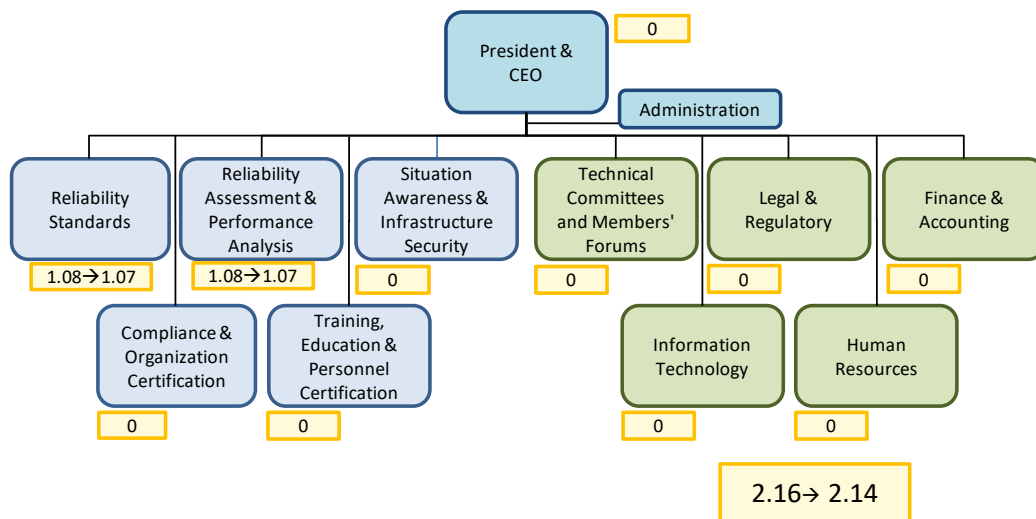
2021 Budget Staff Allocations - RE Division



2020 Budget Staff Allocations - CS Division



2021 Budget Staff Allocations - CS Division



Appendix B Acronyms

This section lists acronyms used in this document.

Acronym	Definition
AI	Audits and Investigations
BAA	Balancing Authority Area
BEP	BES Exception Process
BES	Bulk Electric System
BPS	Bulk Power System
CC	Compliance Committee
CCEP	Criteria Compliance and Enforcement Program
CDAA	CMEP Data Administration Application
CEH	Continuing Education Hour
CGNC	Corporate Governance and Nominating Committee
CMEP	Compliance Monitoring and Enforcement Program
COP	Compliance Oversight Plan
CORC	Compliance Monitoring and Enforcement and Organization Registration and Certification Program
CORES	Centralized Organization Registration ERO System
CUG	Consortium Users Group
DADSWG	Demand Response Availability Data System Working Group
DER	Distributed Energy Resources
DHS	Department of Homeland Security
DOE	Department of Energy
EAP	ERO Event Analysis Process
EIC	Evaluation of Internal Controls
E-ISAC	Electricity Information Sharing and Analysis Center
EPHPIS	Electric Power Human Performance Improvement Symposium
ERAG	Eastern Interconnection Reliability Assessment Group
ERO	Electric Reliability Organization
FAC	Finance and Audit Committee
FERC	Federal Energy Regulatory Commission
FFT	Find, Fix, Track and Report
GADSWG	Generating Availability Data System Working Group
GMD	Geomagnetic Disturbance
HQCMÉ	Hydro-Québec Contrôle des mouvements d'énergie
HSIN	Homeland Security Information Network
IESO	Independent Electricity System Operator
IRA	Inherent Risk Assessment
IRPTF	Inverter-Based Resource Performance Task Force
ISO	Independent System Operator
LMTF	Load Modeling Task Force
LSE	Load Serving Entity
MACD	Market Assessment and Compliance Division
MDCC	Management Development and Compensation Committee
ME	Mitigation and Enforcement
MIDASWG	Misoperation Information Data Analysis System Working Group
MMWG	Multi-Regional Modeling Working Group
MOU	Memorandum of Understanding
NAERM	North American Energy Resilience Model
NAESB	North American Energy Standards Board
NATF	North American Transmission Forum
NBEUB	New Brunswick Energy and Utilities Board
NBMG	Node Breaker Modeling Group

Appendix B

Acronym	Definition
NCCIC	National Cybersecurity and Communications Integration Center
NEL	Net Energy for Load
NERC	North American Electric Reliability Corporation
NLH	Newfoundland and Labrador Hydro
NOI	Notice of Inquiry
NOPR	Notice of Proposed Rulemaking
NPCC	Northeast Power Coordinating Council, Inc.
NSPI	Nova Scotia Power Incorporated
NSUARB	Nova Scotia Utility and Review Board
OEB	Ontario Energy Board
ORCG	Organization Registration and Certification Group
PAS	Performance Analysis Subcommittee
PAWG	Probabilistic Assessment Working Group
PC	Pension Committee
PJM	Pennsylvania-Jersey-Maryland Interconnection LLC., Regional Transmission Organization
PPMVTf	Power Plant Model Verification Task Force
PSWG	Physical Security Working Group
QCMEP	Québec Reliability Standards Compliance Monitoring and Enforcement Program
RAPA	Reliability Assessment and Performance Analysis
RAPA-SG	ERO RAPA Steering Group
RAS	Reliability Assessment Subcommittee
RAS	Remedial Action Scheme
RC	Reliability Coordinator
RCC	Reliability Coordinating Committee
RISC	Reliability Issues Steering Committee
RSC	Regional Standards Committee
RSTC	Reliability and Security Technical Committee
RTWG	Reliability Training Working Group
RTO	Regional Transmission Organization
SAFNR	Situational Awareness-FERC, NERC, Regions
SAIS	Situation Awareness and Infrastructure Security
SAMS	System Analysis and Modeling Subcommittee
SAR	Standards Authorization Request
SCPS	Standards Committee Process Subcommittee
SDT	Standards Drafting Team
SPCS	System Protection and Control Subcommittee
SMS	Synchronized Measurement Subcommittee
SPIDERWG	System Planning Impacts from Distributed Energy Resources Working Group
SPS	Special Protection Systems
TADSWG	Transmission Availability Data System Working Group
TFCO	Task Force on Coordination of Operation
TFCP	Task Force on Coordination of Planning
TFE	Technical Feasibility Exception
TFIST	Task Force on Infrastructure Security and Technology
TFSP	Task Force on System Protection
TFSS	Task Force on System Studies
UFLS	Underfrequency Load Shedding

Appendix C Index of Figures and Tables

		Table to be Inserted		

From: [Guy V. Zito](#)
To: [Ruida Shu](#)
Subject: FW: [EXTERNAL] Aggregated Starter Topics/Questions
Date: Wednesday, January 20, 2021 10:55:20 AM

Include the email below in the RSC agenda package for Brad's participation.

From: Bradley E. Nelson <bradley.nelson@inl.gov>
Sent: Wednesday, January 20, 2021 10:18 AM
To: Guy V. Zito <gzito@npcc.org>
Cc: randy.crissman@nypa.gov
Subject: FW: [EXTERNAL] Aggregated Starter Topics/Questions

CAUTION - EXTERNAL EMAIL

Do not click on links or open any attachments unless you recognize the sender and know the contents are safe.

Hi Guy:

Thanks for the discussion we had towards the end of 2020. As discussed here are the general areas of questions we are interested in hearing more about from energy sector participants relative to grid communications.

Thanks,
Brad

Topic Area	Example Questions
Current operational communication network architecture / domains	• How is communications engineering organized in your company? Are there different organizations for IT and OT networks? • Are communications systems designed, implemented, and maintained internally or outsourced? • Describe your OT network architecture or topology (WAN, FAN , etc.)? • Do you have shared network components between enterprise and operational technologies (e.g. multi-service WAN)? • Does your organization have policy for private communication infrastructure? • What percentage do you own vs lease? • Do you own any private RF spectrum? • Do you have your own fiber infrastructure? • Do you have your own microwave infrastructure? • Do you interchange data over Internet links? If so, what? • What RF expertise do you have?

Grid modernization initiatives/strategies	• What operational use cases does your organization currently employ (AMI, distribution automation, etc.)? • What new use cases are in your strategy or are exploring? • What is the current level of visibility in your distribution system? • Are you seeing significant DER integration on your system? • Are there regulatory mandates or incentives for DER? • Are you exploring distributed intelligence, distributed controls?
Existing management systems and models	• Please describe your current management systems. ◦ How do you maintain your electric network model (GIS, CIM)? ◦ Is the current network state always available digitally? ◦ EMS? DMS? ADMS? DERMS? OMS? AMI? Asset Management? • How do you maintain your communication network model (e.g. GIS, Autocad)? • Do you have an accurate inventory of your assets?
Emerging needs for communications technology to support advanced grid strategies	• What changes do you anticipate are required in your network to support future grid strategies? • How do you determine the requirements for the communication systems that support the grid strategy? • How do you select new technologies from the many choices? • Do you perform RF propagation analysis in house? ◦ Do you possess an accurate RF interference model of your entire territory? ◦ Do you have an accurate terrain model (with elevation) for your entire territory? • How is funding approved and allocated? • What process do you use to plan network expansion and improvements? ◦ How do you measure performance of the communication systems? ◦ How to you prioritize reliability improvements? • Who allocates funding to communications systems and projects? • What percentage of budget is dedicated to communication systems? • Do you have any new systems planned in your grid mod strategy?
Lessons learned from past projects involving communication technology	• What are some successes that you have had deploying communication technology? • What are some failures?

deployment	• Are there any organizational changes that may have helped or were there any that hurt? • Are there tools or processes that would have improved the project?
Process for coordinating communication system multi-year plans with T&D multi-year plans	• How does the group fulfill planning on the communications side? • What level of coordination do you have with transmission and distribution planning? • How does this planning intersect with capital planning of the utility (substation, transmission, distribution, metering, system operations • (Design, Implementation, Operation, Support) How do you deal with legacy technology and integrating new technology? Is this part of a strategy?
Existing tools utilized to assess current communication network performance and analyze future needs	• Do you have or are investigating any network planning tools? • Do you use RF modeling software? • What tools are used and what kind of monitoring do you perform on your OT and IT networks? • Are electric operation management systems and communication operational management systems integrated at all? • Have you been thinking about any tools for this area? If so, which ones?

Brad Nelson
509-919-1838