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 #20-2

May 13, 2020 12:00 p.m. – 4:00 p.m. EST **WebEx Meeting**

May 14, 2020 8:30 a.m. – 2:00 p.m. EST **WebEx Meeting**

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

Day 1 - RSC Business:
Guest Code: 640902731
Password: GEpMbg5i@22 (43762454 from phones)

Day 2 - DER Forum:
Guest Code: 649052018
Password: EKmnt3VT$79 (35668388 from phones)

Day One RSC Business:

For Reference:
Glossary of Terms Used in NERC Reliability Standards, dated February 24, 2020
NPCC Glossary of Terms, dated January 14, 2014

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

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 @ 1:00PM	10/17/18 (F)	10/17/18 (I)
Project 2016-02 Modifications to CIP Standards Norm Dang from IESO @ 1:15PM	12/16/19 (F)	4/6/20 (F)
Project 2017-01 Modifications to BAL-003-1.1	4/17/19	10/24/19

David Lemmons from EthosEnergy @ 1:30PM	(I)	(F)
Project 2019-02 BES Cyber System Information Access Management William Vesely from Con-Ed @ 1:45PM	2/3/20 (F)	2/3/20 (I)
Project 2019-03 Cyber Security Supply Chain Risks Tony Hall from DT @ 2:00PM	6/22/20 (F)	6/22/20 (A)
Project 2019-04 Modifications to PRC-005-6 Giannuzzi Giuseppe from HQ @ 2:15PM	8/28/19 (F)	
Project 2019-05 Modifications to PER-003-2 Alison Oswald or SDT Chair @ 2:30PM	8/30/19 (I)	
Project 2019-06 Cold Weather Matthew Harward and Jordan Mallory @ 2:45PM	5/21/20 (F)	
Technical Rationale for Reliability Standards Chris Larson from NERC @ 3:00PM NC	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)	
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 *SPS*
(Status of RAS Implementation/Transition)
5.1.2 Directory#12 Retirement
5.1.3 A-10 Classification of BPS Elements
5.1.4 Directory#1 A-10 Conforming Changes
5.1.5 Directory#5 and A10 Errata
5.1.6 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 22nd – Call	February 19th – Call	March 19th – Atlanta GA (NERC)
April 22nd – Call	May 20th – Call	June 17th – Denver, CO (Xcel Energy)
July 22nd – Call	August 19th – Call	September 24th – Salt Lake City, UT (WECC)
October 21st – Call	November 19th – Call	December 9th – 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 - Meeting
November 4-5 - Meeting		

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 three 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

10.0 Other Items of Interest

10.1 NPCC Board of Directors Meeting (BOD) 2019

January 29th – SGR Law Offices, Jacksonville, FL	March 18th - Call	May 6th – NPCC Office
June 3rd – Call	June 24th – NPCC Office	August 5th – Call
September 2nd and 3rd – Toronto, Ontario	October 28th – Call	December 2nd – Albany, NY

10.2 NPCC 2021 Business Plan and Budget Schedule

10.3 Executive Order on Securing the United States Bulk-Power System

11.0 Future RSC Meetings and Conference Calls

11.1 RSC 2020 Meeting Date

February 12th-13th, NPCC Office at New York NY
May 13th-14th, WebEx
August 5th-6th, Hydro Quebec at Montreal Quebec
October 14th-15th, IESO or Hydro One at Toronto Ontario
December 3rd General Meeting Albany NY

Day Two DER Forum:

May 14, 2020 8:30 a.m. – 2:00 p.m. EST

12.0 Distributed Energy Resources (DER) Forum Topics

12.1 DER, Approach to Regional Guidance and DER Impact Reporting
12.2 EPRI Presentation by Devin Van Zandt and Jens Boemer at 9:00 AM
12.3 The Joint Utilities of New York Presentation by David Conroy at 10:00 AM
12.4 Presentation by Vandan Divatia from Eversource
12.5 DER Impact on UFLS presentation by Dan Kopin from Utility Services 11:30 AM
12.6 Autonomous Energy Grids – A vision of Highly Distributed Future by Benjamin Kroposki from NREL at 11:00 AM

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 #20-1
February 12, 2019 10:00 a.m. – 4:00 p.m. EST
February 13, 2019 8:30 a.m. – 2:00 p.m. EST
NPCC Office
Board Room
1040 Avenue of Americas 10th Floor
New York, NY
Attire: Business Casual

Dial-In: 415-655-0003 (USA) / 416-915-6530 (Canada)
Day 1 - RSC Business:
Guest Code: 644911024
Password: HeF5pM8* (43357680 from phones)

Day 2 - DER Forum:
Guest Code: 649478554
Password: Eni2bT*7 (36422807 from phones)

Day One RSC Business:

For Reference:
Glossary of Terms Used in NERC Reliability Standards, dated August 12, 2019
NPCC Glossary of Terms, dated January 14, 2014

	Name	Organization	Sector(s)	Day(s)	Comment
1.	Guy Zito	Northeast Power Coordinating Council		1 & 2	
2.	Gerry Dunbar	Northeast Power Coordinating Council		1 & 2	
3.	Ruida Shu	Northeast Power Coordinating Council		1 & 2	
4.	Kal Ayoub	FERC	Guest	1 & 2	
5.	Howard Gugel	NERC	Guest	1 & 2	
6.	Al McMeekin	NERC	Guest	1 & 2	
7	Chantal Mazza	Hydro Quebec	2	1 & 2	Via WebEx
8.	Nicolas Turcotte	Hydro Quebec	1	1 & 2	
9.	Herb Schrayshuen	Power Advisors, LLC - Proxy for NextEra Energy, LLC	4	1 & 2	
10.	Chris Overberg	Consolidated Edison Co. of New York, Inc.	3	1 & 2	
11.	Cristhian Godoy	Consolidated Edison Co. of New York, Inc.	5	1 & 2	

12.	Deidre Altobell	Consolidated Edison Co. of New York, Inc.	1	1	
13.	Payam Farahbakhsh	Hydro One Networks	1	1 & 2	
14.	Brian Robinson	Utility Services, Inc.	5	1	
15.	Sean Lagan	IESO	2	1 & 2	
16.	Mike Cooke	Ontario Power Generation	4	1 & 2	
17.	Constantin Chitescu	Ontario Power Generation	4	1 & 2	
18.	Randy Crissman	NYPA	Guest	1 & 2	
19.	Salvatore Spagnolo	NYPA	4	1 & 2	
20.	Shivaz Chopra	NYPA	6	1	
21.	Jim Grant	NYISO	2	1 & 2	
22.	Mike Jones	National Grid	3	1 & 2	
23.	Sean Bodkin	Dominion Energy Services	4	1 & 2	Via WebEx
24.	Joel Charlebois	AESI	7	1 & 2	
25.	Ben Wu	Orange and Rockland	3	1 & 2	
26.	David Burke	Orange and Rockland	3	1 & 2	Via WebEx
27.	David Kiguel	Independent	7	1 & 2	Via WebEx
28.	Quintin Lee	Eversource	1	1 & 2	
29.	John Pearson	ISO-NE	2	1 & 2	
30.	Vijay Puran	New York State Department of Public Service	6	1 & 2	Via WebEx
31.	Mike Ridolfino	Central Hudson Gas and Electric	1	1 & 2	
32.	Randhir Singh	PSEG	Guest	1 & 2	
33.	Don Nelson	MA State	Guest	1 & 2	Via WebEx
34.	Ken Stell	Vistra Energy	Guest	1	Via WebEx
35.	Francesco Elmi	NPCC	Guest	1	Via WebEx
36.	Aaron Hornick	NPCC	Guest	1	Via WebEx
37.	Norm Dang	IESO	Guest	1	Via WebEx
38.	Mark Atkins	AESI	Guest	1	Via WebEx
39.	Dean Laforest	ISO-NE	Guest	1	Via WebEx
40.	Jordan Mallory	NERC	Guest	1	Via WebEx
41.	Matt Harward	SPP	Guest	1	Via WebEx
42.	Giannuzzi Giuseppe	Hydro Quebec	Guest	1	Via WebEx
43.	William Vesely	Consolidated Edison Co. of New York, Inc.	Guest	1	Via WebEx

44.	Tracy MacNicoll	Utility Services	Guest	1	Via WebEx
45.	Alison Oswald	NERC	Guest	1	Via WebEx
46.	Tony Hall	Project 2018-04 Drafting Team Member	Guest	1	Via WebEx
47.	JoAnn Murphy	Project 2018-04 Drafting Team Member	Guest	1	Via WebEx
48.	David Lemmons	Ethos Energy	Guest	1	Via WebEx
49.	Chris Larson	NERC	Guest	1	Via WebEx
50.	John Allen	SER Phase 2 Drafting Team Member	Guest	1	Via WebEx
51.	Benjamin Loebick	UI	Guest	2	
52.	Andrew Drennen	Landis and Gyr	Guest	2	
53.	Jim Murphy	IESO	Guest	2	
54.	Marianne Blasman	Burlington Hydro	Guest	2	
55.	Ryan Quint	NERC	Guest	2	
56.	Kevin Schneider	Pacific Northwest National Laboratory	Guest	2	Via WebEx
57.	Philip Jonat	WSP USA	Guest	2	
58.	Mayer Sasson	Consolidated Edison Co. of New York, Inc.	Guest	2	

Introductions and Chair's Remarks

Guy Zito provided an update to the RSC members.

- The Standards Efficiency Review (SER) Phase 2 project is underway. ~~SER review and the~~ A SAR will be sent to the NERC Standards Committee involving data reporting and revisions to TOP and IRO standards. ~~going through SC for approval. 17 or 18 requirements are being looked at for TOP standards~~

- A Distributed Energy Resources (DER) position paper is being developed by NERC. NERC needs to define DER. ~~Specific type of energy sources and reliability guidelines. Define DER.~~
- The at-large members of the NERC Reliability and Security Technical Committee (RSTC) have been approved. Six members of the NERC RSTC are from the NPCC Region.
- RSC Vice-Chairs Quintin Lee and Mike Jones will serve another two-year term. ~~It~~This will go to the NPCC board for final approval at their next meeting.
- The RSC executive committee is still looking for a Canadian representative to volunteer.
- The NPCC website is being revised. The new website is expected to be ready at the end of March.

NPCC Antitrust Compliance Guidelines

The NPCC Antitrust Compliance Guidelines were read by Ruida Shu.

Agenda Items:

1.0 Review of Agenda

Approval of Agenda—No revision is necessary to the draft RSC meeting agenda.
Herb Schrayshuen made the motion for approval.
Quintin Lee seconded the motion.
The meeting agenda were approved as read.

2.0 RSC Meeting Minutes

Approval of Minutes—No revision is necessary to the draft RSC meeting minutes of 12-5-19.
Mike Jones made the motion for approval.
Payam Farahbakhsh seconded the motion.
The meeting minutes were approved as read.

3.0 Drafting Team Members and Executive Tracking Summary

3.1 NPCC Members on NERC Drafting Teams
The RSC members reviewed the roster for NPCC members on the NERC Drafting Team and added Devon Tremont to Project 2019-04.

3.2 NERC Project Tracking Spreadsheet
Guy Zito and Ruida Shu provided a brief update on the NERC Project Tracking Spreadsheet.

4.0 Open Action Items

4.1 Open Action Items List
All the action items are completed.

5.0 Items Requiring RSC Discussion

5.1 NERC Weekly Standards Bulletin
Guy Zito reviewed the NERC weekly standards bulletin with the RSC group.

5.2 Updates from the Reliability Coordinating Committee (~~,~~RCC):
Randy Crissman provided an update on his involvement in regards to various activities. A revised A-10 document and implementation plan is in the process of being approved ~~,~~ It is on the RCC agenda for February 27th. A NPCC Member ballot is expected to start on March 1st or 2nd.
The NERC EMP Task Force is in the progress of developing a workplan that prioritizes tasks. The workplan will be sent to the NERC Board. ~~recommendation on the Task Force.~~
They are working on a~~the~~ Task Force charter.
The President issued an executive order on the EMP last month.
DHS has the responsibility to develop a timeline on the executive order.

5.3 NPCC RSC Approved Work Plan 2020-2021
The RSC members reviewed the approved version of the RSC Work Plan 2020-2021.
The NPCC BOD made a minor modification to the RSC Work Plan 2020-2021 on item number 21 added: "for any Standards related recommendations." This was in regard to interaction with the NERC Reliability and Security Technical Committee (RSTC).

Formatted: Superscript
Formatted: Superscript
Formatted: Superscript

5.4 Standards Efficiency Review (SER) Phase 2 SAR by Chris Larson (3:15PM)

Chris Larson and John Allen called in at 3:15PM.

CIP SER team met today. They had their third meeting and reviewed all the industry comments. They are trying to finalize the list of the CIP requirements for retirement.

The CIP SER team identified potential retirement opportunities and provided justifications for the retirement. Two-three months period necessary before the team is ready to post it. The SER team is looking at around 12-15 CIP requirements for retirement but that number will decrease.

The SER O&P team drafted an initial SAR and it is being modified to address appropriate concerns.

The goal is to simplify and reduce the administrative burden on the data exchange.

Some opportunity to clarify the language for industry and maybe some potential consolidation of standards.

Data retention recommendations from the SER has been approved in December 2019. The team made recommendations of five schemes at the December 2019 SC meeting. There are some concerns from FERC on the ROP changes. Risk mitigation framework responsibilities are being assigned to RSTC.

5.5 Supply Chain Next Steps

Howard Gugel from NERC provided a presentation on the Supply Chain on low risk systems.

According to the study, it is recommended to include Electronic access controls for medium and high impact BES Cyber Systems and Physical access controls for medium and high impact BES Cyber System into the Supply Chain Standards.

It is not recommended to include Electronic access monitoring and logging, physical access monitoring and logging and Protected Cyber Assets (PCAs).

The goal is to develop guidelines with CIPC Supply Chain Working Group.

Most low impact assets reside in organizations with higher impact assets.

Many are not planning to apply supply chain risk management plans to low impact assets.

Most low impact assets are individually lowest risk, but a coordinated attack could impact reliability.

Significant percentage of generation resources allow third party access.

Significant percentage of “low-only” transmission stations and substation allow third party access.

It is also recommended to include low impact BES Cyber System with remote electronic access connectivity in future modification of Supply Chain Standards.

NERC is working on a Standard Authorization Request to revise CIP-003.

US Defensive Act discussed by Guy Zito.

Howard Gugel mentioned the additional security risk and concerns on the use of drones.

6.0 NERC Reliability Standards

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

6.1 Currently Posted Projects

Project	Comment Period End Date	Ballot Period End Date
Project 2015-09 Establish and Communicate System Operating Limits Dean Laforest from ISO-NE @ 1:30PM	10/17/18 (F)	10/17/18 (I)
Project 2016-02 Modifications to CIP Standards Norm Dang from IESO @ 1PM	12/16/19 (F)	12/16/19 (A)
Project 2017-01 Modifications to BAL-003-1.1 David Lemmons from EthosEnergy @ 3:00PM	4/17/19 (I)	10/24/19 (F)
Project 2017-07 Standards Alignment with Registration Mark Atkins from AESI @ 1:15PM	12/12/19 (F)	12/12/19 (I)
Project 2018-04 Modifications to PRC-024-2 Tracy MacNicoll from Utility Services @ 2:30PM	11/4/19 (F)	11/4/19 (A)
Project 2019-02 BES Cyber System Information Access Management William Vesely from Con-Ed @ 2:15PM	2/3/20 (F)	2/3/20 (I)
Project 2019-03 Cyber Security Supply Chain Risks Alison Oswald, Tony Hall and JoAnn Murphy from SDT @ 2:45PM	8/1/19 (I)	
Project 2019-04 Modifications to PRC-005-6 Giannuzzi Giuseppe from HQ @ 2:00PM	8/28/19 (F)	
Project 2019-05 Modifications to PER-003-2 Allison Oswald @ 2:45PM	8/30/19 (I)	
Project 2019-06 Cold Weather Jordan Mallory or SDT Chair @ 1:45PM	11/5/19 (F)	
Technical Rationale for Reliability Standards Al McMeekin	12/18/19 (I)	12/18/19 (I)
Comments: (I) – Informal; (F) – Formal; (N) – Nomination Period **Ballots:** (I) – Initial; (A) – Additional; (F) – Final		

Project 2016-02 Modifications to CIP Standards:
Norm Dang called in at 1PM and presented all the latest changes to Project 2016-02. CIP-012-1 is submitted to FERC August 2018, FERC approved it on January 23, 2020.
Tentative effective date likely to be April 1, 2022.
ERO has reviewed the Implementation Guidance and some changes are needed. SDT is updating the IG and will resubmit the IG to ERO.
CIP-002-6: Additional ballot passed on Transmission Owner Control Centers (TOCC) performing Transmission Operator Obligations. The TOCC changes and 2.12 criteria are ~~and it is~~ currently on hold due to inadvertently affect some GO/GOP Control Centers where they are reclassified from low to medium impact.
May need to change 2.12 criteria or a regional variance (WECC or TRE) as well as an additional ballot. NERC is reviewing the issue.
Project 2016-02 SDT will continue with outreach which will include: mini webinars on VCA, SCI, ESZ, Zero Trust, IRA/ERC, Encryption and “What’s in it for me” whitepaper.

One day technical conference for all NERC entity SEMs on April 1, 2020 Atlanta.
The drafting team worked on CIP-005 and Technical Rationale.
They also reviewed comments on ESZ vs ESP, Physical ESP firewalls (EACMS vs SCI) – backwards compatibility and Overloaded SCI definition.
The drafting team removed references to ESP and ESZ from CIP-005, leaving legacy definition for ESP and EAP in place for backward compatibility and modified SCI definition.
Creation of drafts of both Technical Rationale and Implementation Guidance underway for proposed CIP-005, CIP-007 and CIP-010 Standards.
First draft to be finalized for review at February 24, 2020 SDT meeting.

Technical Rationale for Reliability Standards:
Al McMeekin provided a brief summary on the Technical Rationale for Reliability Standards.
The goal for this project is to remove all Implementation Guidance and Technical Rationale from the Standard document itself and put them into one document.
The review team have identified 23 standards qualify for this.
There are two posting and the first posting consists 9 standards (IRO standards)
NERC posted these 9 standards with a non-binding poll.
NERC is looking to post the second group of standards on March 5, 2020 to April 20, 2020. Non-binding poll for the last 10 days. The documents will be split into Implementation Guidance and Technical Rationale. (Two documents)

Project 2015-09 Establish and Communicate System Operating Limits:
Dean Laforest called in at 1:30PM.
The FAC SDT met in late November 2019 and provided a revised proposal to FERC staff for review in terms of proposed changes to FAC-011, FAC-014 and co~~o~~rresponding changes to TOP-001 and IRO-008.
FERC staff provided useful vetted feedback in early January.
The FAC SDT met in late January 2020, used the feedbacks from FERC, and developed a revised set of standards (FAC-011, FAC-014, TOP-001 and IRO-008, plus minor revisions to other standards where IROL is currently used) for NERC staff for a late March posting. The goal is to receive input from the 45-day comment period.
The next SDT meeting will be around late May 2020 in MISO to review comments and if industry support then the standard will go to ballot.

Project 2019-06 Cold Weather:
Jordan Mallory and Matt Harward called in at 1:45PM.
The SAR addresses recommendation #1 in regards to the FERC and NERC cold weather report.
The goal is to achieve situational awareness for entities during extreme cold weather.
The SDT received many comments on the SAR in regards to potential geographical location, generator type, ambient weather types etc.
Formal response to the comments will be provided and the SDT is in the process of modifying the SAR in order to address the comments.

The intent is not creating any redundancy and the SDT will look into the existing standards for any potential opportunity to modify the existing standard to address the issue.
Two parts to this project: 1. Cold weather preparedness. 2. Communication between entities. It is more focused on the capabilities of the generators rather than the availabilities. Next SAR drafting team meeting is March or April 2020.
The SAR drafting team is looking to finalize the SAR and submit to SC for approval in June 2020.

Project 2019-04 Modifications to PRC-005-6:
Giuseppe Giannuzi called in at 2PM.
The SAR drafting team met on January 2020 and reviewed all the comments on the SAR.
NAGF commented for additional clarity on the SAR in terms of the analog and digital equipment.
The SAR drafting team is looking to expand the SAR from only the AVR to analog and digital control system. The standard should cover any devices that trip or cease injection.
The SAR drafting team is also looking to modify the battery testing portion of the standard. The current table in the standard only applies to certain types of batteries and the team is looking at adding batteries like Lithium ion to the table. They want to make it technology neutral.
Add UFLS only DP into the SAR.
The SAR drafting team will meet again next week to address the remainder SAR and comments.

Project 2019-02 BES Cyber System Information Access Management:
William Vesely called in at 2:15PM.
The SDT is currently reviewing the comments.
The SDT will meet and review the comments at their next SDT meeting end of February 2020.
The SDT is looking to scale back the project and it should address some of the concerns from the comments.
CIP-011 needs update.
There are some concerns where the entities' s relay could be considered as a storage unit.

Project 2018-04 Modifications to PRC-024-2:
Tracy MacNicoll called in at 2:30PM.
The drafting team defined applicable protection and added language: "case injecting current" within R1 and R2.
Quebec variance has different voltage No-Trip Boundaries and it only applies to TOs since there are confirmed Transmission Owners in the Quebec Interconnection that own GSUs.
Planning Coordinators are applicable to Quebec Variance.

The project passed the final ballot on December 13, 2019. It is approved by NERC BOT on February 6, 2020 and it will be submitted to FERC for approval.

Project 2019-03 Cyber Security Supply Chain Risks:
Alison Oswald, Tony Hall and JoAnn Murphy called in at 2:45PM.
FERC Order issued October 18, 2018, directed inclusion of EACMS.
The goal is to make minimal changes to meet the FERC Order 850 and the NERC Supply Chain report.
Changes include adding EACMS and PACS to CIP-005, CIP-010, and CIP-013.
The drafting team is coordinating with the other CIP project teams. (Project 2016-02 and Project 2019-02)

Project 2019-05 Modifications to PER-003-2:
Alison Oswald discussed Project 2019-05 with the members of RSC.
On February 11, 2019, the Personnel Certification Governance Committee (PCGC) posted a whitepaper proposing changes to the NERC System Operator Certification Program.
The four existing credentials would be changed to a single credential.
The Job Task Analysis (JTA) indicated that many job tasks performed within the four certification areas now overlapped.
The transition to single credential would bring the common set of knowledge and skills to better support the Bulk Electric System (BES)
Adopting one credential will enhance and improve reliability by promoting a broader base of knowledge for each NERC Certified System Operator.
This will enable better communication and interaction across all System Operator positions, providing better portability, and produce a well-rounded System Operator.
The drafting team will consolidate the three requirements to a single requirement.
Consider how the knowledge areas determined by the PCGC's JTA were utilized to establish a single credential.
Incorporate these knowledge areas into the areas of competency without creating any possible reliability gaps.
The plan is to have initial posting in April 2020 and July 2020 for additional ballot if required.

Project 2017-01 Modifications to BAL-003-1.1:
David Lemmons called in at 3PM.
The SDT met a couple week ago and discussed the concern (Performance level on the generator).
Phase 2: Performance obligation on the generator and BA creates issues and the drafting team is looking to modify the language.
There is a meeting schedule on the second week of March 2020 at Duke Energy facility Charlette NC.

6.2 Ballot History (Since last RSC Meeting)
Ruida Shu reviewed the Ballot History document in the meeting.

6.3 Comment Form History (Since last RSC Meeting)

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

7.0 NERC Drafting Team Nominations

7.1 Currently Posted Drafting Team Vacancies

7.1.1 None at this time

7.2 Closed Drafting Team Nominations (Since last RSC Meeting)

7.2.1 None at this time

7.3 Solicitation for Informal Development Teams

7.3.1 None at this time

8.0 NPCC Regional Reliability Standards

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

8.1 Current Activities:

8.1.1 PRC-006-NPCC-2 Automatic Underfrequency Load Shedding Standard status update.

The petition for approval is sent to FERC on December 23, 2019 and FERC has assigned Docket RD20-1-000 open for comment period which closed on January 22, 2020.

9.0 NPCC Non-Standards

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

9.1 Items for Discussion:

9.1.1 Directory#7 *SPS*

TFCP and TFSP are continuing their review of Directory#7.
TFCP is reviewing the regional review process and TFSP is reviewing the existing criteria to ensure consistency with Directory#7.
TFCP has set up a series of meetings throughout the spring with other NPCC Task Forces.
TFCP anticipates a first posting in May and a second posting in September in order to have a revised version of D#7 approved by the Full Members by the effective date of PRC -12-2 in January 2021.

(Status of RAS Implementation/Transition)

9.1.2 A-10 Classification of BPS Elements (status of TFCP review).

TFCP approved the revised version of the A-10 in November and a RCC Webinar was conducted in January 2020.
The revised A-10 methodology will be on the RCC agenda for approval in Febraary 2020 and subsequent to RCC approval will be presented to the Full Members for ballot approval.

9.1.3 Executive Tracking Summary

10.0 RSC Member Items of Interest

10.1 RSC Roster

Ruida Shu reviewed the RSC roster with the RSC group.

11.0 Standards Activity Post NERC BOT Approval

(Since last RSC Meeting)

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

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

11.2.1 Order on Five-Year Performance Assessment
Docket No. RR19-7-000
https://ferc.gov/whats-new/comm-meet/2020/012320/E-20.pdf

11.2.2 Transmission Planning Reliability Standard TPL-001-5
Docket No. RM19-10-00
https://ferc.gov/whats-new/comm-meet/2020/012320/E-21.pdf

11.2.3 Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers
Docket No. RM18-20-000; Order No.866
https://ferc.gov/whats-new/comm-meet/2020/012320/E-22.pdf

11.2.4 NERC Standards Efficiency Review
Docket Nos. RM19-16-000 and RM19-17-000
https://ferc.gov/whats-new/comm-meet/2020/012320/E-24.pdf

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

11.4 FERC Sunshine Act Meeting Notice

11.5 FERC Open Meeting Summaries

12.0 NERC Meetings

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

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

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

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

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

12.5 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 - Meeting
November 4-5 - Meeting		

12.6 Reliability Issues Steering Committee (RISC)
http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO_Reliability_Risk_Priorities_RISC_Reccommendations_Board_Approved_Nov_2016.pdf

13.0 NERC Items of Interest (Since last RSC Meeting)

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

13.1.1 There has been one new Lesson Learned issued since the last RSC meeting.

13.2 Alerts
http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx
There has been no new NERC Alerts released since the last RSC meeting.

13.3 NERC Reliability and Security Guidelines
https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

14.0 Other Items of Interest

14.1 NPCC Board of Directors Meeting (BOD) 2019

January 29th – SGR Law Offices, Jacksonville, FL	March 18th - Call	May 6th – NPCC Office
June 3rd – Call	June 24th – NPCC Office	August 5th – Call
September 2nd and 3rd – Toronto, Ontario	October 28th – Call	December 2nd – Albany, NY

14.2 NPCC and ERO 2020 Business Plan and Budget Schedule

15.0 Future RSC Meetings and Conference Calls

15.1 RSC 2020 Meeting Date

February 12th-13th, NPCC Office at New York NY
May 13th-14th, NY-ISO at Saratoga NY
August 5th-6th, Hydro Quebec at Montreal Quebec
October 14th-15th, IESO or Hydro One at Toronto Ontario
December 3rd General Meeting Albany NY

Day Two DER Forum:

	Name	Organization	Comment
1.	Brandon Brynarski		
2.	Brian Robinson	Utility Services	
3.	Brian Yung		
4.	Dan V		
5.	David Lovelady		
6.	Michael Lombardi	NPCC	
7.	Michael Porcaro		
8.	Ray Joyce		
9.	Zachary Gallagher		
10.	Chantal Mazza	Hydro Quebec	
11.	Donald Nelson	MA State	
12.	Nicolas Compas		
13.	Casey Kirkpatrick		
14.	David Kiguel	Independent	
15.	Gabriel Adam		
16.	Junji Yamaguchi	Hydro Quebec	
17.	Ken Stell	Vistra Energy Corp.	
18.	Laura Mcleod	NB Power	

19.	Enakpodia Agbedia		
20.	Eric Henderson		
21.	Charles Alonse		
22.	Hao Fu		
23.	Hung Huynh		
24.	Mark Gaines		
25.	Matthew Koenig		
26.	Michael Billheimer	NPCC	
27.	Neeraj Lal	NPCC	
28.	Nurul Abser	NP Power	
29.	Per-Anders Lof	National Grid	
30.	Susmit Patel		
31.	Tony Napikosky		
32.	Yves Albert		
33.	Zhu Chuanjiang (Chelsea)		
34.	Bradley Marszalkowski		
35.	Aaron Anaya		
36.	Brian Shanahan	National Grid	
37.	CB PSEGLI		
38.	Chris Overberg	Con-Edison	
39.	Humi		
40.	Matt Cloud		
41.	Rudi		
42.	Anas		
43.	Doug Ayer		
44.	ISO Engagement		
45.	Jalpa Patel		
46.	Jason Pause	NY State	
47.	Joel Charlebois	AESI	
48.	Keith Burrell		
49.	Kevin Schneider		
50.	Nick Parrotta	PLM	
51.	Nicolas Turcotte	Hydro Quebec	
52.	Payam	Hydro One	
53.	Stephen Wemple		
54.	Tracy MacNicoll	Utility Services	
55.	Samer Arafa		

16.0 Distributed Energy Resources (DER) Forum Topics

16.1 DER, Approach to Regional Guidance and DER Impact Reporting

Guy Zito welcomed attendees to the DER forum and highlighted the role of NPCC in his opening remarks. He noted the NPCC BOD interest in DER and that NPCC as a region will examine ways to better coordinate activity and identify any reliability

gaps that may exist as a result of DER proliferation. He reminded the attendees that a DER reporting form is currently available for stakeholder use in addressing issues that may arise as result of DER installations.
Guy Zito stated that Version 1 of the NPCC DER Guidance document is currently posted on the NPCC website and that the Regional Standards Committee (RSC) will be working with stakeholders throughout 2020 in order to develop a Version 2 of the document which will incorporate additional comments and concerns received during the development of Version 1.

16.2 NERC SPIDERWG and IRPTF Presentation by Ryan Quint from NERC
Ryan Quint provided an update on NERC DER activities including the Inverter Based Resource Performance Task Force (IRPTF) and the System Planning Impacts of Distributed Energy Resources Working Group (SPIDERWG).
He noted that inverter-based resources connected to the BES are subject to IEEE P2800 while distribution level DER resources are governed by IEEE 1547-2018.
Ryan Quint reported that the National Association of Regulatory Utility Commissioners (NARUC) has approved a motion to adopt the IEEE 1547 -2018.
The NERC IRPTF examines DER issues directly impacting the BES and develops disturbance reports and alerts to disseminate to industry.
The IRPTF also produces reliability guidelines and modelling studies.
Mr. Quint provided background on the activities of the SPIDERWG and noted that aggregate amounts of distribution level DER will impact the BPS.
Mr. Quint highlighted the adoption of IEEE 1547-2018 from a BPS reliability perspective.
The SPIDERWG has also developed a reliability guideline on the impact of the adoption of IEEE 1547-2018.
Mr. Quint described the organization of the SPIDERWG and its separate focus areas of modeling, verification, studies and coordination.
IEEE P2800 which includes inverter-based resources, covers all BPS and BES transmission level and sub transmission level.
IEEE 1547-2018 includes all power producing resources on distribution level.
NERC Inverter-Based Resource Performance Task Force (IRPTF) is working on IBR Modeling Studies Report, Fast Frequency Response Fundamentals white paper, NERC Reliability Standards Review for IBR white paper, EMT Modeling Studies Reliability Guideline, Modeling Studying BPS-Connected Energy Storage/Hybrid Plants Reliability Guideline and Energy Transition to Increasing Penetration of BPS-connected Inverter-Based Resources Technical Report.
NERC System Planning Impacts of Distributed Energy Resources Working Group (SPIDERWG) is working on analyzing the aggregate amounts of DER and how they can impact the BPS.
Adoption of IEEE 1547-2018 and coordination necessary for successful IEE 1547-2018. The working group drafted a Reliability Guideline on the adoption of IEEE 1547-2018.

16.3 AMI and Smart Meters Presentation by Benjamin Loebick from UI
Mr. Loebick of United Illuminating presented on U.I.'s advanced metering program
Mr. Loebick provided background on the technologies and milestones that have led to U.I.'s current state of Advanced Metering Infrastructure. (AMI)U.I.'s AMI

technology currently facilitates better billing and access to consumption information, energy efficiency, outage communications and demand response options. Big data supported by AMI is leveraged by U.I. in order to monitor customer voltage and local transformer loading. AMI will be critical in evaluating the impact of DER deployment on the distribution system and customer usage patterns. U.I. anticipates that full AMI deployment will facilitate outage restoration and system design improvements.
UI's foundational technologies & applications are customer focused, grid enabling and can be leveraged with enhancements to move the distribution grid to stages 2 and 3. (AMI, OMS, GIS, SAP, SCADA, PL Historia, etc.)
The new Advanced Metering Infrastructure (AMI) enable an economy-wide transition to a renewable future by decarbonization of power generation, transportation and building heating and cooling sectors. They address reliability and resilience standards system-wide, and deploy or enhance the utilization of AMI to provide customers with a more resilient, reliable and secure commodity.
They also address energy affordability for all Connecticut ratepayers residential, commercial and industrial customers.
UI started their automated meter reading from 1999-2002, upgraded AMI communications from 2009-2019 and advanced meters deployment from 2019-2024.
UI utilized the new AMI technology for their outage detection and response. By utilizing the new AMI system UI is able to reduced their outages duration.
The AMI technology also provided theft detection capabilities and O&M cost savings.
Daily and time of use (TOU) usage and rates available to the customers.
The existing telecommunications backbone also enhances Cybersecurity.
AMI also provides access to invaluable data analytics that can unlock benefits. (Voltage events, distribution transformer monitoring etc.)
UI has completed 2 Distribution Automation (DA) pilots to test communications ahead of broader deployment.
AMI technology is required for grid modernization in Connecticut, it also enables customer expectation and energy objectives.

16.4 AMI and Smart Meters in Ontario presentation by Jim Murphy IESO (9-9:30AM)
Jim Murphy of the IESO presented on the smart metering initiative in Ontario. Mr. Murphy noted that the IESO operates as a big data machine that oversees Ontario's electricity market, operates the power system in real time and utilizes smart metering as part of its effort to promote efficiency and plan for the future. He described the milestones that led to the IESO being designated as he Smart Meter Entity (SME) in Ontario. In 2019 the SME reached a milestone of over 5 million smart meters installed. MR. Murphy provided background on Time of Use (TOU) pricing including summer and winter on peak and off-peak pricing tiers. Jim provided an overview of how the Meter Data Management Repository works in conjunction with a Local Distribution Company's metering and billing systems to provide accurate information to support TOU billing. He described how the value of the data can be

further enhanced by enabling government policy initiatives and energy efficiency programs. He provided details on Time of Use (TOU) structure in Ontario.
Jim discussed Ontario's Smart Metering System and their Smart Metering Entity.
He provided details on MDM/R in numbers, Architecture, Privacy and Security.
IESO utilized and enhanced the data provided by the AMI system.
Following the 2016 OEB orders, the IESO embarked on an effort to unlock the value from the data it collects through the MDDM/R to create efficiencies, build new value streams and to reduce costs for electricity consumers.
Access to the smart meter big data can enable advancements in government policy initiatives, research, energy efficiency programs and industry innovation.
IESO established the value proposition.

16.5 AMI and Smart Meters Presentation by Marianne Blasman from Burlington Hydro (9:30-10AM)

Marianee Blasman of Burlington Hydro presented on advanced mater infrastructure (AMI) in Ontario. She described Burlington Hydro's strategy for the transition to smart meters and the IESO's Meter Data Management Repository (MDMR). Ms. Blasman provided an overview of the separate and critical information systems that were required to be integrated as part of the AMI effort. Ms. Blasman provided background on operational data systems that represent a central repository for large volumes of data including electrical consumption and operational alarms. Ms. Blasman highlighted areas of ongoing change including cyber intrusion, cyber countermeasures and the existing regulatory climate.
She provided information on strategy for transition to Smart Meters. Some of the strategies are alignment of key information systems, recognize roles/responsibilities of these systems, achieve streamlined system integration and make sure you get the data.
Meter Data Management & Operational Data Store Repository (MDM-ODS)is big data, central repository for large volume of data that belongs in an integrated Customer Information and Billing Systems(CIS)-MDM-ODS System.
The benefits of MDM-ODS which is meter/network health, seamless integration with centralized IESO's MDM/R and allows for integrated outage management system.
The challenges of MDM-ODS are understanding the true potential and role of an integrated MDM-ODS, establishing new proactive business process that are smart, efficient and automated across systems, processing large volume of information in a

timely and effective manner to make data useable and data organization/dashboard presentation.
Marianne also discussed their smart meter deployment process and the challenges.

16.6 OpenFMB presentation by Kevin Schneider from Pacific Northwest National Laboratory (11:00-11:30AM)

Kevin Schneider provided an overview of increasing distribution system resilience using flexible DER and micro grid assets.
The Open Field Message Box (Open FMB) translates the information from different communication protocols and allows sharing of this information.
Open FMB was developed in response to the proliferation of DER and other smart technologies and the need for greater interoperability.
Utility communication systems are typically based on a centralized model so that information from distribution systems still has to be routed through centralized energy management systems. By removing the need for communications to route through a centralized system the utility's ability to manage the distribution system is improved.
Kevin Schneider highlighted a 3-day event attended by industry stakeholders and vendors designed to demonstrate Open FMB interoperability.
OpenFMB is a project design to increase distribution resiliency though flexible operating strategies. This will be accomplished by actively engaging utility and non-utility assets as flexible resources.
Project Objectives: Develop flexible operating strategies that integrate centralized and decentralized control systems, engage utility and non-utility assets to increase the resiliency of critical end-use loads to all hazards events and develop, deploy, a layered control architecture using commercial-off-the-shelf (COTS) equipment and open source code.
Kevin discussed approaches, key issues and distinctive characteristics.
The architecture of OpenFMB is a layered control structure with elements of a laminar control architecture developed to coordinate self-healing, microgrids, and DERs.
Concept of Operations (CONOPS) has been completed, including 12 use-cases.
Before equipment can be operationally deployed, the architecture, controls, and set points must be developed, simulated, and validated. A multi-stage validation approach has been taken.
The OpenFMB "Harness" is the physical realization of the reference architecture.
Early Open FMB work used commodity Raspberry PI prototype controllers. The utility assets for this project will use COTS RTUs and/or 4G LTE gateways, with OpenFMB in a containerized environment. Using open-software containerized applications on COTS equipment enables hardening for industrial applications, while ensuring interoperability and portability. COTs devices integrate TPM2.0 crypto-chips and X.509 certificates with whitelisted, containerized, OpenFMB applications.
COTs devices are being tested on the initial harness implementation.

The Meeting is adjourned at 12:37PM on February 13, 2020.

Respectfully Submitted,

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

Northeast Power Coordinating Council, Inc. (NPCC)

Antitrust Compliance Guidelines

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

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

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

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

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

Any NPCC meeting participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NPCC's antitrust compliance policy is implicated in any situation should call NPCC's Assistant Secretary, Ruta Skučas, Esq. at 1-202-530-6428.

Public Announcement

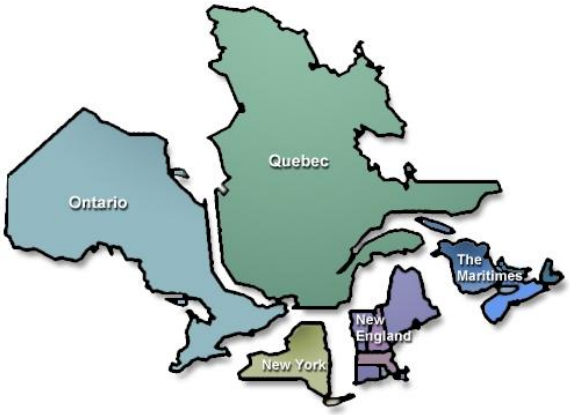
RSC and DER Forum Meetings, WebEx, and Conference calls:
Participants are reminded that this meeting, WebEx, and conference call are public. The access number was posted on the NPCC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members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

NPCC, Inc.

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

DRAFT

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 12/XX/2020

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

Contributors

John Pearson	**ISO-NE**
Brad Marszalkowski	**ISO-NE**
David Forrest	**EPRI Consultant**
Ryan Quint	**NERC**
David Conroy	**Joint Utilities of New York-CMP**
Herb Schrayshuen	**Power Advisors on behalf of NextEra**
James Grant	**NYISO**
Brian Robinson	**Utility Services**
Dan Kopin	**Utility Services**
Michael Jones	**National Grid (RSC Co-Vice Chair)**
Quintin Lee	**Eversource (RSC Co-Vice Chair)**
Benjamin Loebick	**United Illuminating**
Guy V. Zito	**NPCC (RSC Chair)**

NPCC also thanks the Regional Standards Committee 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 and various enhancements and clarifications and Appendices**

Contents

Executive Summary 4
Introduction and Objective 5
NPCC DER Impact Reporting 7
DER BPS Impact Considerations 7
NPCC Interconnection Guidance 8
- Voltage Response 10
- Frequency Support 11
- Reconnection to the Utility System 12
- Inverters 12
- Certification per UL 1741 SA as grid support utility interactive inverters 13
- Minimum Protective Functions 14
- Metering 15
- Power Quality 17
- Power Factor 17
- Islanding 17
- Automatic Underfrequency Load Shedding (UFLS) Programs 17
- Effective Grounding for DER 18
- Resource Adequacy 18
- Energy Storage Systems for DER 19
- System control and Data Acquisition (SCADA) and Communications 20

DER Recommendations 20
Appendix A, NPCC DER Impact Reporting Form and Process 22
Appendix B, NPCC Areas- Comparisons 24
Appendix C – SPIDER Working Group Reliability Guidelines & Activities 25
Appendix D, NPCC Reliability Principles 28
Appendix E, State and Provincial AGIR Information 32
- New York State 32
- New England, by State 32
- Province of Quebec (some references are only available in French) 35
- Province of Ontario 38
- Province of New Brunswick 39

Appendix F, ISO New England 40

Appendix G, State Renewable and Green Energy Requirements 42

Commented [HS1]: Add a section on Resource Adequacy modelling after Effective GRounding

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 risks[1] to the BPS, recommendations to mitigate them, and also identifies opportunities to leverage the operational characteristics of DER to enhance reliability and resilience of the NPCC Bulk Power System (BPS). Helpful links to other resources are provided throughout the document.

As Distributed Energy Resources (DER) installed on the distribution system, 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"[2] 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 national efforts 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 are either developed, or in the process of being developed, by the NERC System Planning Impacts Working Group (SPIDER), along with links to some of their documents. NPCC and its members have been engaged in efforts at the national level and are leading efforts to address outstanding issues within the scope of those groups and provide expertise. With the understanding of what efforts are underway nationally, 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. Specifically, in the area of 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.

[1] 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,

[2] "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, analyze and determine a way to address any issues. 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 is purely informational and as NERC's SPIDER, 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 Labs, the Electric Power Research Institute 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 generating resources are included in DER is not broadly accepted by the industry. Also, DER is not currently a term that is defined by NERC.

For the purpose of this NPCC guidance, 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, irrespective of capacity, allowing individual small 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 would not include individual rooftop solar or wind turbines or other localized DER net metering installations, however the aggregate effect of these types of DER can have a significant change in 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 21[3]. NPCC is now observing aggregation of DER beginning to enter capacity wholesale markets within the NPCC Region. This document will continually 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 improvement and address potential reliability risks, promote good utility interconnection practices necessary for reliability, and promulgate

[3] 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 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.

information on how DER can enhance reliable operation of 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 as well as the Joint Utilities group of NY to align processes where possible.

National standards are established to address DER impact on system reliability. IEEE Std 1547-2018 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 through inclusion in those interconnection agreements.

As DER continues to penetrate 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 and influence the effect of these DER resources on the BPS. It is important to understand how DER is interconnected, planned, operated and how they interact with the transmission system.

Reliably and securely integrating DER into the electric system requires a comprehensive multi-pronged approach utilizing perspectives from different areas. 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 formulation 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 nature of the system within which 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 contemporary DER is theoretically capable of bringing several enhancements to reliability, provided that there are sufficient design specifications and interconnection requirements to implement the enhancements. Inverter based DER may use fast, programmable response to provide benefits to reliability if properly configured with coordination 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
- Under frequency 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.

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. EPRI has an open sourced co-simulation tool under test. 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.

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 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 reliablity issues and opportunities for further work, and provide general guidance and information where possible, offer consistent guidance with North America wide technical direction to promote reliable interconnection and operation of DER. It is recognized that DER may not be placed optimally and 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 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 availability and quality of forecasting.
- Observability and situational awareness of DER and importance of implementing Advanced Metering Infrastructure (AMI) if telemetry is not deployed
- DER impacts on Underfrequency Load Shed programs.
- Impacts of DER on the 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 others 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 guidance[4]. The level of detail and specificity provided is intended to be used as 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 are encouraged to reach out directly to other 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 for the simulated transmission event, the transmission system could become unreliable for that event and require remediation. This can occur in several scenarios such 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.

[4] At the time of this guidance document development, these include but are not limited to: NERC (e.g. SPIDER WG, IRPTF, Events Analysis, Modelling and Standards process), Inverter- Based Resources Task Force), IEEE (IEEE Std 1547-2018, P2800), and various state initiatives such as the New York ITWG, Other Regional, Provincial and State initiatives.

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 coordinate with NERC standard PRC-24-02. 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 ensuring a reliable transmission system at the lowest possible cost.

IEEE 1547-2018 was approved in 2019 and also unanimously adopted by the National Association of Regulatory Utility Commissioners (NARUC). The standard outlines the technical specifications and performance requirements which are universally needed for interconnection and interoperability of DER and will 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 the 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 and standards.

The DER owner must follow interconnection agreements and any AGIR requirements for fault ride through. Utilities and other AGIR entities should ensure that their requirements describe necessary DER performance with ride-through capabilities for frequency and voltage events. Interconnection agreements and standards generally have requirements to provide documentation upon request.

In terms of 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 standards 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 must be capable of automatically disconnecting the generation from the system to which it is directly connected upon detection of frequency or voltage conditions outside of the applicable ride-through requirements. Note that those interconnection agreements and standards should account for both distribution protection and reliability of the BPS. For three-phase installations, the over and under voltage function should be included for each phase and the over and under frequency protection on at least one phase. All phases of a generator or inverter interface should disconnect for appropriate voltage or frequency trip conditions sensed by the protective devices. Voltage protection should be wired phase to ground for single phase installations

and for applications using wye grounded-wye grounded service transformers. 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 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 Process[5].

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 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 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 band of voltage levels will ensure that DER do not prematurely trip and further deteriorate system conditions. IEEE Std. 1547-2018 includes ranges of 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.

[5] At this time there has not been an assessment of potential change in sensitivity (increase or decrease) to the effects of GMD from the presence of high DER penetration. This is a potential reliability risk to be evaluated in the future.

Quebec Interconnection

Ride through during system disturbances is of primary importance for resources connected to the grid, with the objective of maintaining system reliability[6]. 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 distribution resources 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. The sequence for a protective device to automatically initiate a disconnect sequence from the utility system is also detailed in the most current version of 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 is a need to establish a mechanism to ensure distribution provider transmit information to planners and operators as to which DER facilities are connected to distribution feeder that have UFLS protection systems.

Quebec Interconnection

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 DER must be capable of riding through frequency as low as 55.5 Hz (for a short time period). Therefore

[6] NERC report on Loss of Wind Turbines During System Disturbances : NERC Report-Loss of Wind Turbines

in Quebec, UFLS systems must operate outside this operating rang in accordance with the Quebec variance to the PRC-006-NPCC UFLS-1 regional standard table 4.

Reconnection to the Utility System

If the generation facility is disconnected as a result of the operation of a protective device, the DER owner's equipment must 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.

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, 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 changes direct current (DC) to alternating current (AC). The inverter itself does not produce any 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 bands for voltage ride-through capabilities that are attainable by inverter-based systems where there 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 EPS and to provide increased BPS reliability by further reducing the potential loss of DER during bulk system events.

Inverters intended to provide local grid support during system events that result in voltage and/or frequency excursions as described in this document and should be provided with the required onboard 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 standards and agreements also typically refer to IEEE Std. 1547-2018 functional requirements and include protection setting review requirements.

ISO-NE also has developed a technical bulletin, contained in **Appendix F**, which outlines required settings for inverters in New England.

Certification per UL 1741 SA as grid support utility interactive inverters

Because Inverters certified for IEEE 1547-2003 do not currently provide adequate grid support functionality, in the interim period while IEEE P1547.1-2018 is not yet revised and published, 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. 1547-2018 (2nd ed.)1 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.
- Abnormal performance capability (ride-through) requirements for inverter-based applications should have the ride-through capability per abnormal performance Category II of IEEE Std. 1547-2018 (2nd ed.) as quoted in Tables III and IV. Additionally, an effort is underway at IEEE to

amend 1547-2018 to expand the range of under-voltage trip settings in Category III. If the amendment is approved, Category III inverters should be recommended for use.

Minimum 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 distributed generation facility

• Voltage level of the interconnection

• Location of the distributed generation facility on the circuit

• Distribution transformer

• Distribution system configuration

• Available fault current

• Load that can remain connected to the distributed generation facility under isolated conditions

• Amount of existing distributed generation 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 will 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 the generating equipment.

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 DG 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)[7]. 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.

[7] 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.

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.

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). Net Energy Metering should be required when a DER has the capability or potential to provide generation back into the utility distribution system, however, the eligibility of a DER provider to receive net metering will be subject to the rules of the interconnecting utility and the local regulatory authority that has jurisdiction.

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. 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 reliably 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

The requirements for acceptable flicker levels should be in accordance with the latest version of IEEE Std. 1453 Recommended Practice for the Analysis of Fluctuating Installations on Power Systems. Short and long-term perception of flicker should be within the planning and compatibility levels delineated in any applicable requirements or standards.

Power Factor

If the output power factor, as measured at terminals of the generator, does not meet the connecting utility's power factor requirements, the method of power factor correction necessitated by the installation of the generator can be negotiated with the utility as a commercial item. If the average power factor of the DER over time is proven to be outside 0.9 (leading or lagging) by the customer and accepted by the utility, that power factor range may be used for any further utility facility design calculations and requirements.

Induction power generators may be provided with a VAR capacity from the utility system. The installation of VAR correction equipment by the generator- owner on the DER owner's side of the PCC is to be reviewed and approved by the interconnecting utility prior to installation.

Islanding

The guidance provided in this document is designed and intended to avoid islanding and may be superseded by local requirements. Additional protection schemes and system modifications may be necessary based on the capacity of the proposed system and the configuration and existing loading on the subject circuit.

The need for zero sequence voltage and direct transfer trip protection schemes should be evaluated based on minimum loads on the associated feeder and substation bus, including the impact of fault conditions resulting from DER installation to protect facilities for an islanded condition.

Transfer trip is needed in some instances (e.g. on DER connections to non-radial transmission or sub-transmission circuits) in order to protect the utility systems and DER facility from damage during faults and/or reclosing operations into faults. The decision as to the applicability of direct transfer trip and specific technology to be used form direct transfer trip communications rests with the connecting utility.

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 control operation designed to stabilize BPS islands for a generation deficiency. Various fractions of load are shed through this process, typically 25%. UFLS is primarily installed on distribution feeders, where DER is increasingly being deployed.

NERC has a set of requirements in the PRC-006 standard and NPCC has more stringent requirements in NPCC's Regional Standard, PRC-006-NPCC 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

With the onset of high penetrations of DER, such as photovoltaic (PV) generation, utilities should consider interconnection of PV plants 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 plants are considered voltage-controlled current sources during faults. Inverter-based plants generally provide less short-circuit current than similarly sized synchronous unit.

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.

Resource Adequacy

Forecasting resource adequacy is an import system reliability function. The reporting of generation capability and 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 planners and system operators. Any requirements associated with this information should be in Interconnection Agreements or Tariffs prior to any commissioning of the DER. There are currently no mechanisms within NERC Standards or NPCC Criteria to require DER entities to provide this information. It currently needs to be covered under other contractual agreements such as local utility Interconnection Agreements or Tariffs.

Commented [HS2]: I put this here as a placeholder. More can be said if needed.

Energy Storage Systems for DER

Battery storage technology is undergoing a rapid evolution from Lead Acetate 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 "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 below, the capability of an inverter can be exceeded by the capability of the DER behind it. This is designed with due consideration of the degradation of DER, such as a solar panel over time.

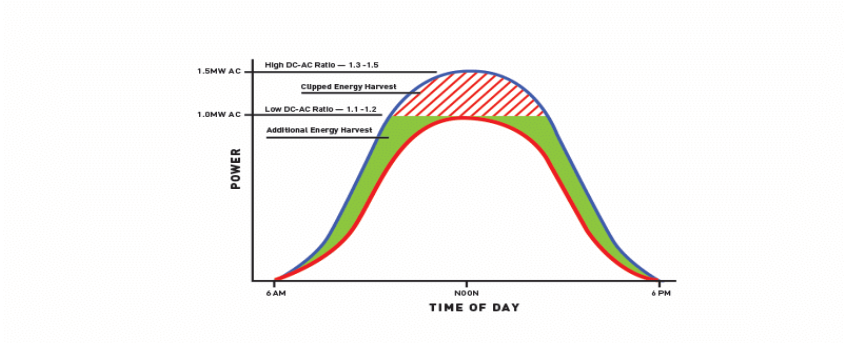


Figure 1- Storage showing Clipped and Unused Energy

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 emergent or planned outage situations. Some NPCC Members have encountered difficulty with obtaining information and data from the DER. 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. 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.

DER Recommendations

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

Participation in National DER Forums

1) Participate in national efforts to fully understand the issues and best practices associated with DER.
2) Engage NPCC and its members at the national level leading efforts to address the issues and provide expertise.
3) As the understanding at the national level 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 generating resources, 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 problem 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 stakeholder.
9) Avoid placement of UFLS on distribution feeders with DER unless sufficient telemetry exists to ensure proper functionality of the UFLS program as a whole.

<u>Planning Related Recommendations Due to Changing Resource Mix</u>

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 BPS[8]
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.

<u>Analytics and simulation recommendations to deal with increase system complexity</u>

10) Support interconnection wide inertia loss study efforts, to determine potential reliability impacts, as DER replaces conventional synchronous generation resources.
11) 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.

[8] 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.

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 to; npccstandard@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.

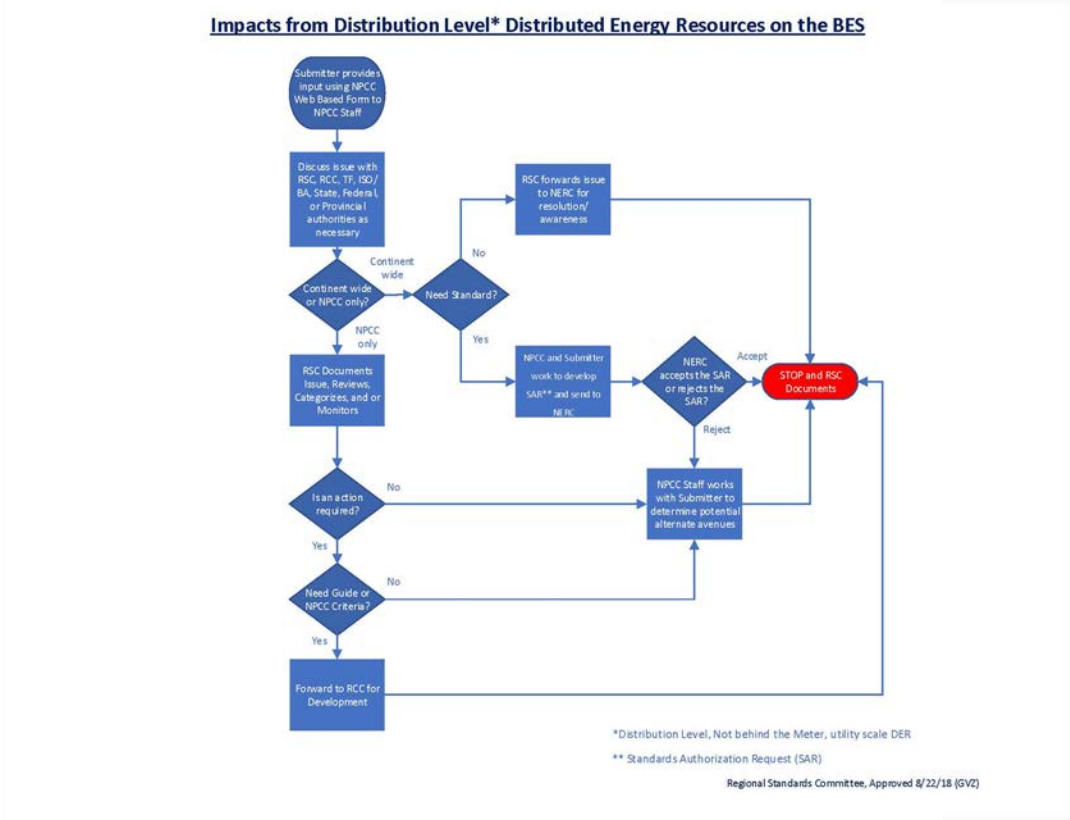
Root Cause or additional Analysis

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



Appendix B, NPCC Areas-Comparisons

Key Inverter based specification extracts

	ISO-NE Inverter Requirements	NG ESB 756 B, C, D	NY SIR[9]	IESO F2 Technical Requirements

[9] NY SIR is the New York Standardized Interconnection Requirement.

Inverter Certification	yes	yes	yes	yes
Voltage and frequency trip settings for inverter-based applications	yes	yes	yes	yes
Voltage Response	yes[10]	yes	yes	yes
Frequency Response	yes[11]		yes	yes
Abnormal performance capability (ride-through) requirements for ~~inverter based~~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	

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

[10] 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

[11] 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

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"[12]:

> **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.

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)

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

	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 Criteria[13], 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

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

requirements. NPCC's core Reliability Principles[14] 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 region[15]. These critical facilities collectively are identified as the NPCC Bulk Power System[16,17].
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 operation[18] 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 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."

[14] The Reliability Principles were summarized in the NPCC 2018 Strategic Review Report.
[15] 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.
[16] 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.
[17] 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
[18] 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. "

6. **Resilience has always been an element of NPCC Criteria:** Based on experience, resilience[19] [20] 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

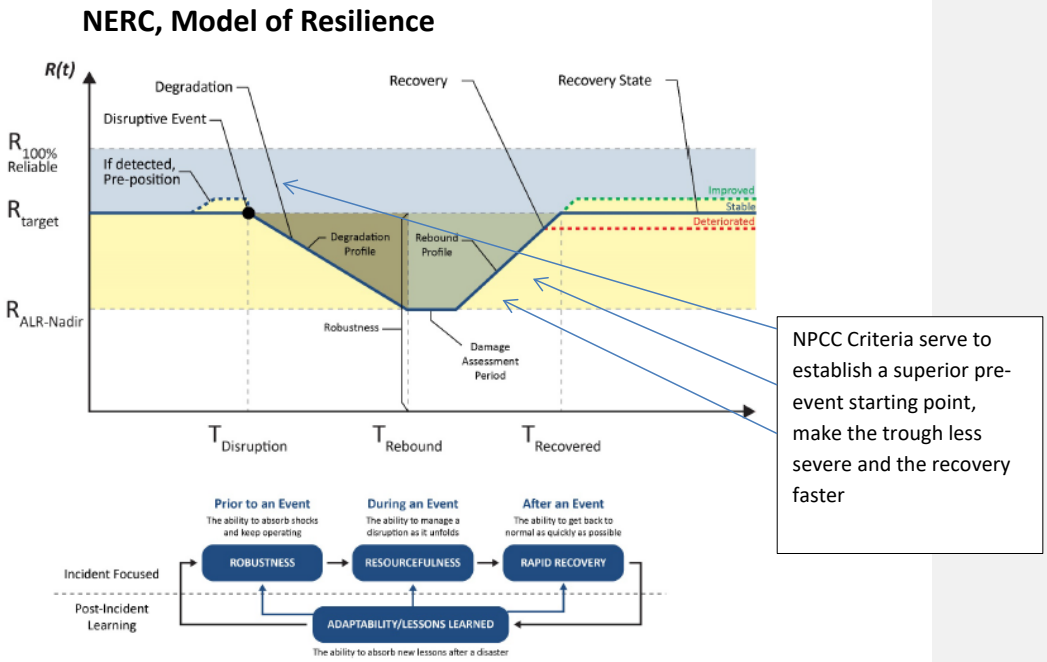


Figure 2.1

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

[19] 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.
[20] In 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".

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 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 (HQCMÉ) 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.

We know you also contacted Hydro-Québec in this matter, but just in case, 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

As noted above, 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

Ènergie 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 (2nd ed.) Category II					
Shall Trip Function	Required Settings		Comparison to IEEE Std 1547-2018 (2nd 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 (2nd 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 (2nd ed.) for Category II
V > 1.20	Cease to Energize	N/A	0.16	Identical
1.175 < V ≤ 1.20	Permissive Operation	0.2	N/A	Identical
1.15 < V ≤ 1.175	Permissive Operation	0.5	N/A	Identical
1.10 < V ≤ 1.15	Permissive Operation	1	N/A	Identical

0.88 ≤ V ≤ 1.10	Continuous Operation	infinite	N/A	Identical
0.65 ≤ V < 0.88	Mandatory Operation	Linear slope of 8.7 s/1 p.u. voltage starting at 3 s @ 0.65 p.u.: $T_{VRT} = 3\text{ s} + \frac{8.7\text{ s}}{1\text{ p. u.}}(V - 0.65\text{ p.u.})$	N/A	Identical
0.45 ≤ V < 0.65	Permissive Operation [a,b]	0.32	N/A	See footnotes a & b
0.30 ≤ 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:

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

b. 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 (2nd ed.) for Category II
f > 62.0	No ride-through requirements apply to this range		Identical
61.2 < f ≤ 61.8	Mandatory Operation	299	Identical
58.8 ≤ f ≤ 61.2	Continuous Operation	Infinite	Identical
57.0 ≤ 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 Requirements

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

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-3

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 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.

4.1.1.2 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

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by the Planning Coordinator or Transmission Planner, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

See Implementation Plan for CIP-014-3.

6. Background:

Reliability Standard CIP-014-2 addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of

such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be

developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.

- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or

- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

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 during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner 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.

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, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an	or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an	result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection	stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						primary control center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	October 1, 2015	Effective Date	New
2	April 16, 2015	Revised to meet FERC Order 802 directive to remove “widespread”.	Revision
2	May 7, 2015	Adopted by the NERC Board of Trustees	
2	July 14, 2015	FERC Letter Order in Docket No. RD15-4-000 approving CIP-014-2	

Guidelines and Technical Basis

Section 4 Applicability

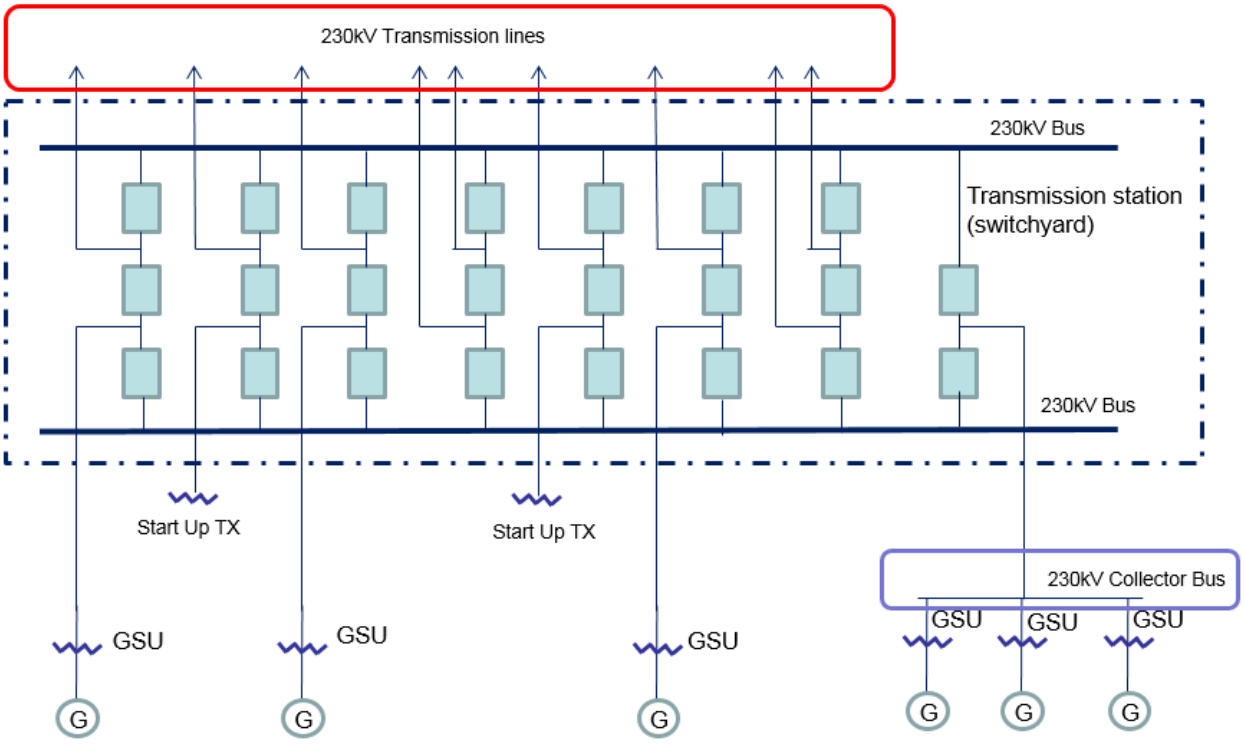
The purpose of Reliability Standard CIP-014 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause instability, uncontrolled separation, or Cascading within an

Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in instability, uncontrolled separation, or Cascading. The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers that, if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission 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 (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. The requirement is not to require identification of, and thus, not intended to bring within the scope of the standard a Transmission station or Transmission substation unless the applicable Transmission Owner determines through technical studies and analyses based on objective analysis, technical expertise, operating experience and experienced judgment that the loss of such facility would have a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged. In the November 20, 2014 Order, FERC reiterated that "only an instability that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1." The Transmission Owner may determine the criteria for critical impact by considering, among other criteria, any of the following:

- Criteria or methodology used by Transmission Planners or Planning Coordinators in TPL-001-4, Requirement R6
- NERC EOP-004-2 reporting criteria
- Area or magnitude of potential impact

The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be

helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center “operationally controls” a Transmission station or Transmission substation when the control

center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk

assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.

- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various

sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

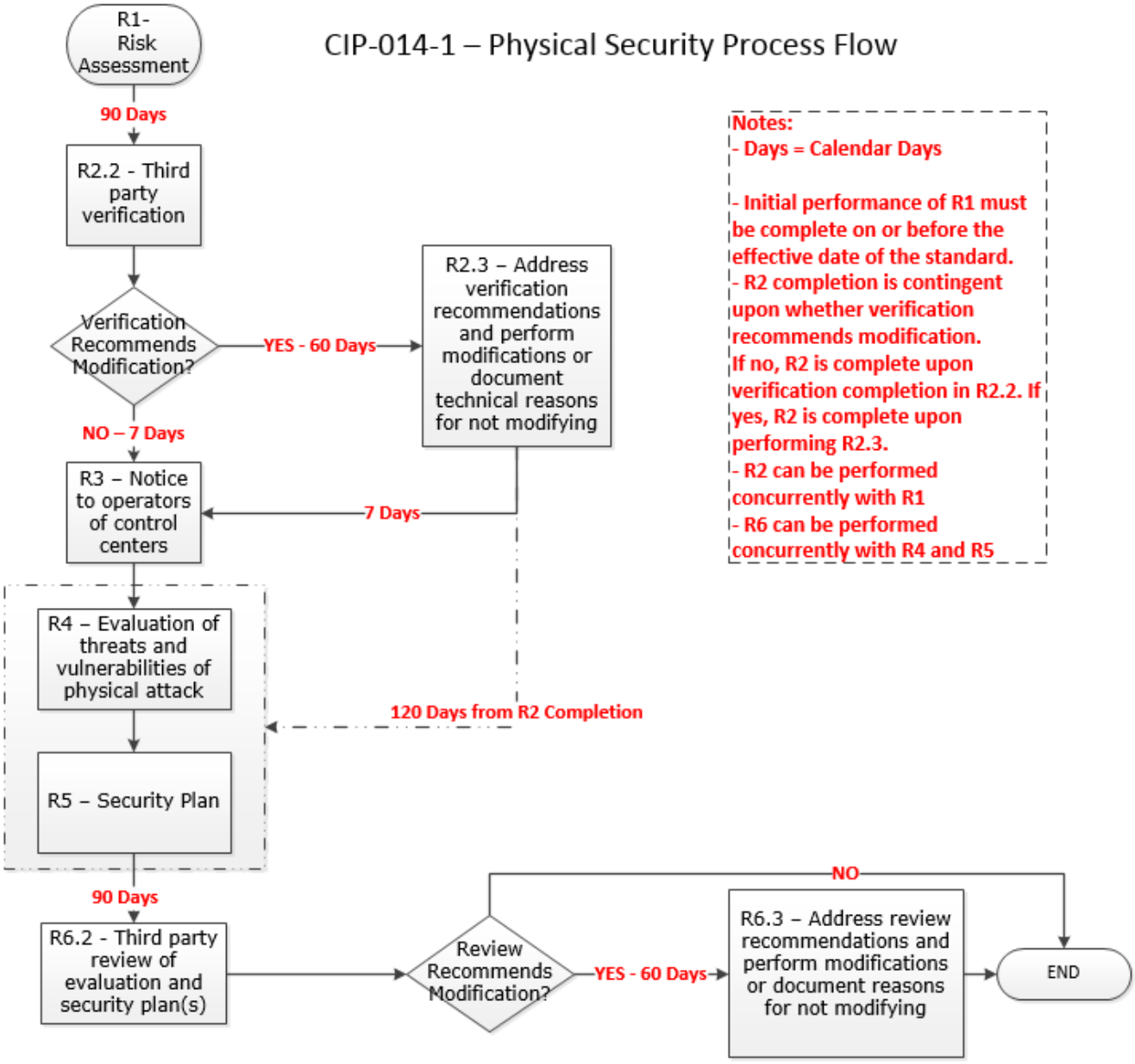
- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
7 Days
R3 – Notice to operators of control centers
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
NO
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

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:
This requirement meets the FERC directive from paragraph 6 of its March 7, 2014 order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through instability, uncontrolled separation, or cascading failures. The requirement is not intended to bring within the scope of the standard a Transmission station or Transmission substation unless the applicable Transmission Owner determines through technical studies and analyses based on objective analysis, technical expertise, operating experience and experienced judgment that the loss of such facility would have a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged. In the November 20, 2014 Order, FERC reiterated that "only an instability that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1." The Transmission Owner may determine the criteria for critical impact by considering, among other criteria, any of the following:

- Criteria or methodology used by Transmission Planners or Planning Coordinators in TPL-001-4, Requirement R6
- NERC EOP-004-2 reporting criteria
- Area or magnitude of potential impact

Requirement R1 also meets the FERC directive for periodic reevaluation of the risk assessment by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

Rationale for Requirement R2:
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term "unaffiliated" is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

Rationale for Requirement R3:
Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

Rationale for Requirement R4:
This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security

plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

Rationale for Requirement R5:
This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Rationale for Requirement R6:
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Physical Security

2. **Number:** CIP-014-32

3. **Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

4. **Applicability:**

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 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.

4.1.1.2 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

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by the ~~its Reliability Coordinator,~~ Planning Coordinator~~,~~ or Transmission Planner, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation ~~as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies~~.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

See Implementation Plan for CIP-014-32.

6. Background:

~~This~~ Reliability Standard CIP-014-2 addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of

such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be

developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.

- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or

- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

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 during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner 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.

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, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an	or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an	result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection	stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						primary control center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	October 1, 2015	Effective Date	New
2	April 16, 2015	Revised to meet FERC Order 802 directive to remove “widespread”.	Revision
2	May 7, 2015	Adopted by the NERC Board of Trustees	
2	July 14, 2015	FERC Letter Order in Docket No. RD15-4-000 approving CIP-014-2	

Guidelines and Technical Basis

Section 4 Applicability

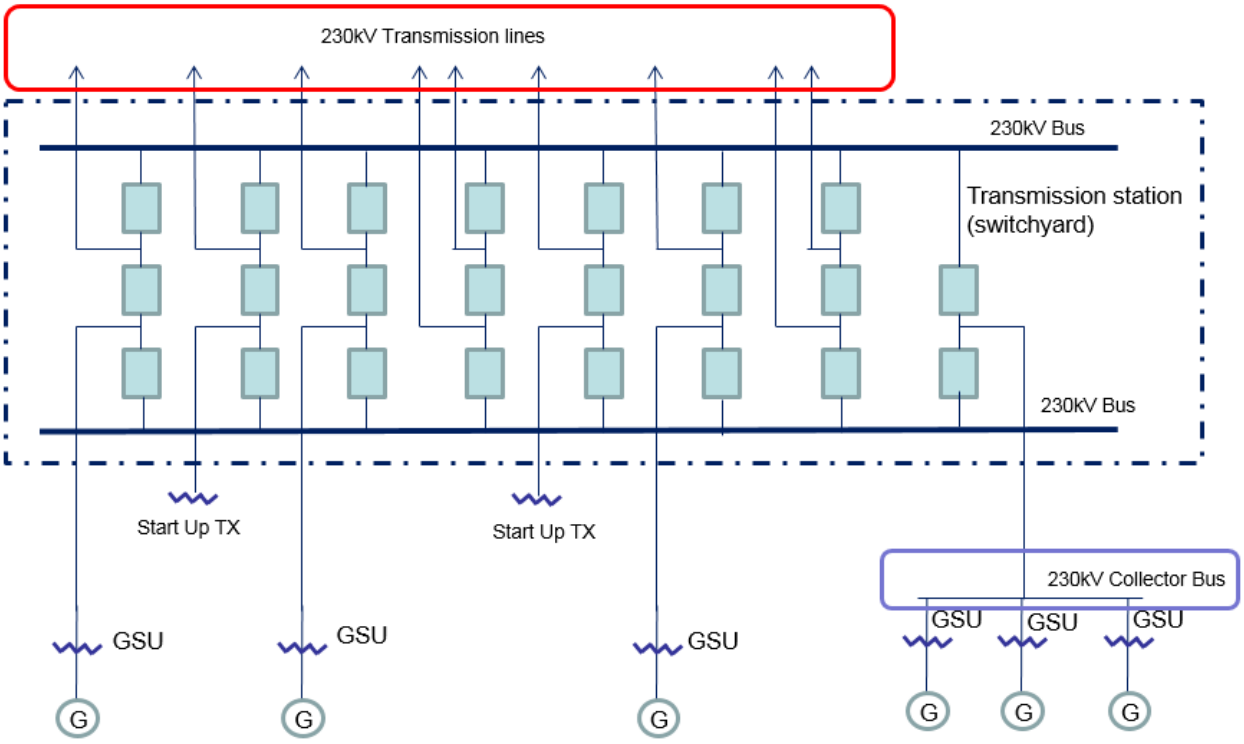
The purpose of Reliability Standard CIP-014 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause instability, uncontrolled separation, or Cascading within an

Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in ~~exceeding one or more Interconnection Reliability Operating Limits (IROLs)~~instability, uncontrolled separation, or Cascading. The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers that, if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission 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 (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. The requirement is not to require identification of, and thus, not intended to bring within the scope of the standard a Transmission station or Transmission substation unless the applicable Transmission Owner determines through technical studies and analyses based on objective analysis, technical expertise, operating experience and experienced judgment that the loss of such facility would have a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged. In the November 20, 2014 Order, FERC reiterated that "only an instability that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1." The Transmission Owner may determine the criteria for critical impact by considering, among other criteria, any of the following:

- Criteria or methodology used by Transmission Planners or Planning Coordinators in TPL-001-4, Requirement R6
- NERC EOP-004-2 reporting criteria
- Area or magnitude of potential impact

The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be

helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control

center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk

assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.

- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various

sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

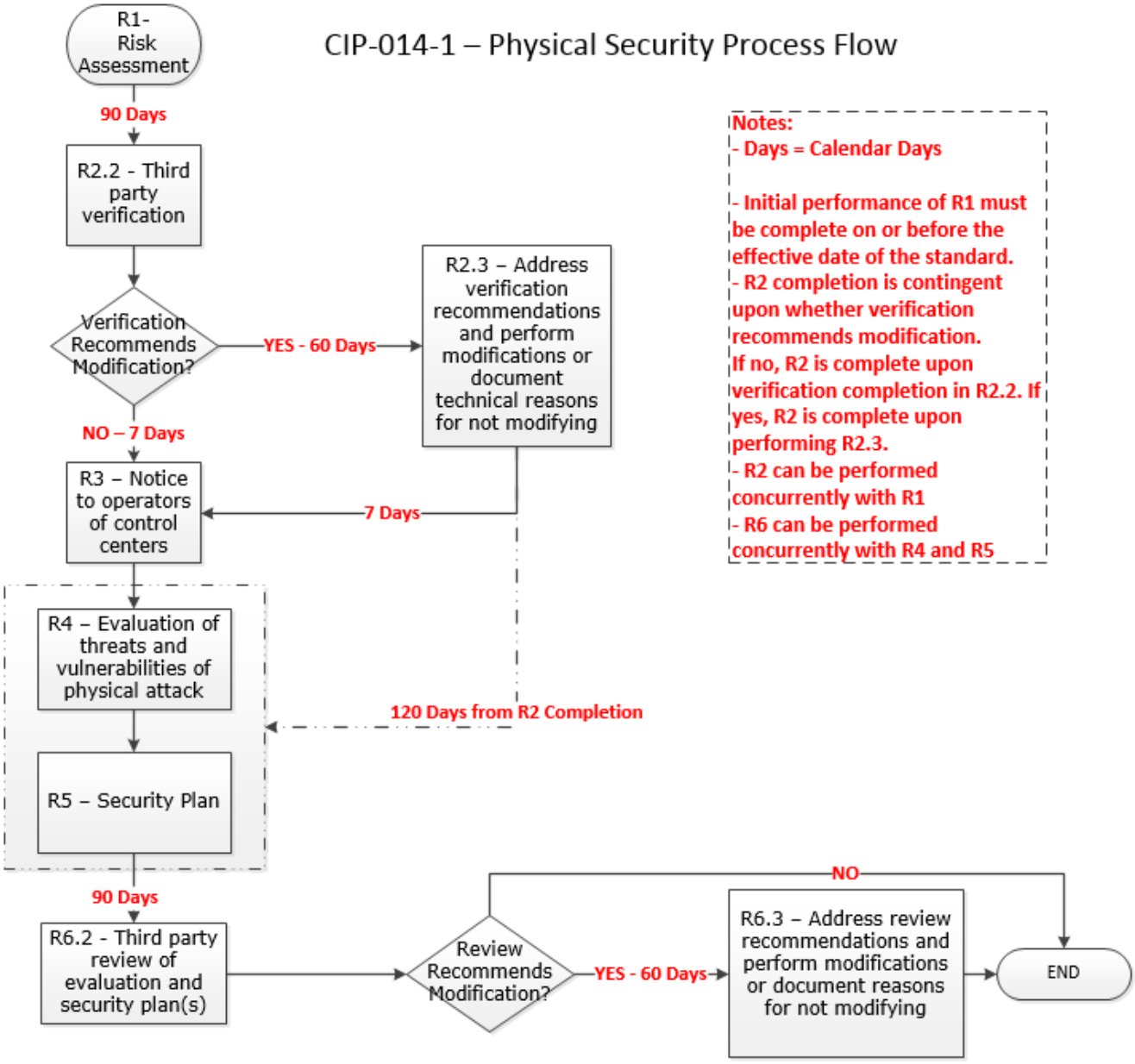
- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
7 Days
R3 – Notice to operators of control centers
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
NO
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

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:
This requirement meets the FERC directive from paragraph 6 of its March 7, 2014 order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through instability, uncontrolled separation, or cascading failures. The requirement is not intended to bring within the scope of the standard a Transmission station or Transmission substation unless the applicable Transmission Owner determines through technical studies and analyses based on objective analysis, technical expertise, operating experience and experienced judgment that the loss of such facility would have a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged. In the November 20, 2014 Order, FERC reiterated that "only an instability that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1." The Transmission Owner may determine the criteria for critical impact by considering, among other criteria, any of the following:

- Criteria or methodology used by Transmission Planners or Planning Coordinators in TPL-001-4, Requirement R6
- NERC EOP-004-2 reporting criteria
- Area or magnitude of potential impact

Requirement R1 also meets the FERC directive for periodic reevaluation of the risk assessment by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

Rationale for Requirement R2:
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term "unaffiliated" is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

Rationale for Requirement R3:
Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

Rationale for Requirement R4:
This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security

plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

Rationale for Requirement R5:
This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Rationale for Requirement R6:
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** Transmission Vegetation Management

2. **Number:** FAC-003-5

3. **Purpose:** To maintain a reliable electric transmission system by using a defense-in-depth strategy to manage vegetation located on transmission rights of way (ROW) and minimize encroachments from vegetation located adjacent to the ROW, thus preventing the risk of those vegetation-related outages that could lead to Cascading.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Applicable Transmission Owners

   4.1.1.1. Transmission Owners that own Transmission Facilities defined in 4.2.

   4.1.2. Applicable Generator Owners

   4.1.2.1. Generator Owners that own generation Facilities defined in 4.3.

   4.2. Transmission Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[1], state, provincial, public, private, or tribal entities:

   4.2.1. Each overhead transmission line operated at 200kV or higher.

   4.2.2. Each overhead transmission line operated below 200kV, identified by the Planning Coordinator or Transmission Planner, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as a Facility that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation.

   4.2.3. Each overhead transmission line operated below 200 kV identified as an element of a Major Western Electricity Coordinating Council (WECC) Transfer Path in the Bulk Electric System by WECC.

   4.2.4. Each overhead transmission line identified above (4.2.1. through 4.2.3.) located outside the fenced area of the switchyard, station or substation and any portion of the span of the transmission line that is crossing the substation fence.

[1] EPAct 2005 section 1211c: *"Access approvals by Federal agencies."*

4.3. Generation Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[2], state, provincial, public, private, or tribal entities:

4.3.1. Overhead transmission lines that (1) extend greater than one mile or 1.609 kilometers beyond the fenced area of the generating station switchyard to the point of interconnection with a Transmission Owner's Facility or (2) do not have a clear line of sight[3] from the generating station switchyard fence to the point of interconnection with a Transmission Owner's Facility and are:

4.3.1.1. Operated at 200kV or higher; or

4.3.1.2. Operated below 200kV and are identified by the Planning Coordinator or Transmission Planner, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as a Facility that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation.; or

4.3.1.3. Operated below 200 kV identified as an element of a Major WECC Transfer Path in the Bulk Electric System by WECC.

5. Effective Date: See Implementation Plan

6. Background: This standard uses three types of requirements to provide layers of protection to prevent vegetation related outages that could lead to Cascading:

a) Performance-based defines a particular reliability objective or outcome to be achieved. In its simplest form, a results-based requirement has four components: *who, under what conditions (if any), shall perform what action, to achieve what particular bulk power system performance result or outcome?*

b) Risk-based preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: *who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?*

c) Competency-based defines a minimum set of capabilities an entity needs to have to demonstrate it is able to perform its designated reliability functions. A competency-based reliability requirement should be framed as: *who, under what conditions (if any), shall have what capability, to achieve what particular result or*

[2] *Id.*

[3] "Clear line of sight" means the distance that can be seen by the average person without special instrumentation (e.g., binoculars, telescope, spyglasses, etc.) on a clear day.

outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the bulk power system?

The defense-in-depth strategy for Reliability Standards development recognizes that each requirement in a NERC Reliability Standard has a role in preventing system failures, and that these roles are complementary and reinforcing. Reliability Standards should not be viewed as a body of unrelated requirements, but rather should be viewed as part of a portfolio of requirements designed to achieve an overall defense-in-depth strategy and comport with the quality objectives of a Reliability Standard.

This standard uses a defense-in-depth approach to improve the reliability of the electric Transmission system by:

- Requiring that vegetation be managed to prevent vegetation encroachment inside the flash-over clearance (R1 and R2);
- Requiring documentation of the maintenance strategies, procedures, processes and specifications used to manage vegetation to prevent potential flash-over conditions including consideration of 1) conductor dynamics and 2) the interrelationships between vegetation growth rates, control methods and the inspection frequency (R3);
- Requiring timely notification to the appropriate control center of vegetation conditions that could cause a flash-over at any moment (R4);
- Requiring corrective actions to ensure that flash-over distances will not be violated due to work constrains such as legal injunctions (R5);
- Requiring inspections of vegetation conditions to be performed annually (R6); and
- Requiring that the annual work needed to prevent flash-over is completed (R7).

For this standard, the requirements have been developed as follows:

- Performance-based: Requirements 1 and 2
- Competency-based: Requirement 3
- Risk-based: Requirements 4, 5, 6 and 7

Requirement R3 serves as the first line of defense by ensuring that entities understand the problem they are trying to manage and have fully developed strategies and plans to manage the problem. Requirements R1, R2, and R7 serve as the second line of defense by requiring that entities carry out their plans and manage vegetation. Requirement R6, which requires inspections, may be either a part of the first line of defense (as input into the strategies and plans) or as a third line of defense (as a check of the first and second lines of defense). Requirement R4 serves as the final line of defense, as it addresses cases in which all the other lines of defense have failed.

Major outages and operational problems have resulted from interference between overgrown vegetation and transmission lines located on many types of lands and ownership situations. Adherence to the standard requirements for applicable lines on any kind of land or easement, whether they are Federal Lands, state or provincial lands, public or private lands, franchises, easements or lands owned in fee, will reduce and manage this risk. For the purpose of the standard the term "public lands" includes municipal lands, village lands, city lands, and a host of other governmental entities.

This standard addresses vegetation management along applicable overhead lines and does not apply to underground lines, submarine lines or to line sections inside an electric station boundary.

This standard focuses on transmission lines to prevent those vegetation related outages that could lead to Cascading. It is not intended to prevent customer outages due to tree contact with lower voltage distribution system lines. For example, localized customer service might be disrupted if vegetation were to make contact with a 69kV transmission line supplying power to a 12kV distribution station. However, this standard is not written to address such isolated situations which have little impact on the overall electric transmission system.

Since vegetation growth is constant and always present, unmanaged vegetation poses an increased outage risk, especially when numerous transmission lines are operating at or near their Rating. This can present a significant risk of consecutive line failures when lines are experiencing large sags thereby leading to Cascading. Once the first line fails the shift of the current to the other lines and/or the increasing system loads will lead to the second and subsequent line failures as contact to the vegetation under those lines occurs. Conversely, most other outage causes (such as trees falling into lines, lightning, animals, motor vehicles, etc.) are not an interrelated function of the shift of currents or the increasing system loading. These events are not any more likely to occur during heavy system loads than any other time. There is no cause-effect relationship which creates the probability of simultaneous occurrence of other such events. Therefore these types of events are highly unlikely to cause large-scale grid failures. Thus, this standard places the highest priority on the management of vegetation to prevent vegetation grow-ins.

B. Requirements and Measures

R1. Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the Minimum Vegetation Clearance Distance (MVCD) of its applicable line(s), operating within their Rating and all Rated

Electrical Operating Conditions of the types shown below[4] *[Violation Risk Factor: High] [Time Horizon: Real-time]*:

1.1. An encroachment into the MVCD as shown in FAC-003-Table 2, observed in Real-time, absent a Sustained Outage,[5]

1.2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,[6]

1.3. An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage[7],

1.4. An encroachment due to vegetation growth into the MVCD that caused a vegetation-related Sustained Outage.[8]

M1. Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R1. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments. (R1)

R2. [Reserved for future use]

2.1.

M2. [Reserved for future use]

R3. Each applicable Transmission Owner and applicable Generator Owner shall have documented maintenance strategies or procedures or processes or specifications it uses to prevent the encroachment of vegetation into the MVCD of its applicable lines that accounts for the following: *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]:*

3.1. Movement of applicable line conductors under their Rating and all Rated Electrical Operating Conditions;

---

[4] This requirement does not apply to circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner subject to this Reliability Standard, including natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, wind shear, fresh gale, major storms as defined either by the applicable Transmission Owner or applicable Generator Owner or an applicable regulatory body, ice storms, and floods; human or animal activity such as logging, animal severing tree, vehicle contact with tree, or installation, removal, or digging of vegetation. Nothing in this footnote should be construed to limit the Transmission Owner's or applicable Generator Owner's right to exercise its full legal rights on the ROW.

[5] If a later confirmation of a Fault by the applicable Transmission Owner or applicable Generator Owner shows that a vegetation encroachment within the MVCD has occurred from vegetation within the ROW, this shall be considered the equivalent of a Real-time observation.

[6] Multiple Sustained Outages on an individual line, if caused by the same vegetation, will be reported as one outage regardless of the actual number of outages within a 24-hour period.

[7] *Id.*

[8] *Id.*

3.2. Inter-relationships between vegetation growth rates, vegetation control methods, and inspection frequency.

M3. The maintenance strategies or procedures or processes or specifications provided demonstrate that the applicable Transmission Owner and applicable Generator Owner can prevent encroachment into the MVCD considering the factors identified in the requirement. (R3)

R4. Each applicable Transmission Owner and applicable Generator Owner, without any intentional time delay, shall notify the control center holding switching authority for the associated applicable line when the applicable Transmission Owner and applicable Generator Owner has confirmed the existence of a vegetation condition that is likely to cause a Fault at any moment *[Violation Risk Factor: Medium] [Time Horizon: Real-time].*

M4. Each applicable Transmission Owner and applicable Generator Owner that has a confirmed vegetation condition likely to cause a Fault at any moment will have evidence that it notified the control center holding switching authority for the associated transmission line without any intentional time delay. Examples of evidence may include control center logs, voice recordings, switching orders, clearance orders and subsequent work orders. (R4)

R5. When an applicable Transmission Owner and an applicable Generator Owner are constrained from performing vegetation work on an applicable line operating within its Rating and all Rated Electrical Operating Conditions, and the constraint may lead to a vegetation encroachment into the MVCD prior to the implementation of the next annual work plan, then the applicable Transmission Owner or applicable Generator Owner shall take corrective action to ensure continued vegetation management to prevent encroachments [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].

M5. Each applicable Transmission Owner and applicable Generator Owner has evidence of the corrective action taken for each constraint where an applicable transmission line was put at potential risk. Examples of acceptable forms of evidence may include initially-planned work orders, documentation of constraints from landowners, court orders, inspection records of increased monitoring, documentation of the de-rating of lines, revised work orders, invoices, or evidence that the line was de-energized. (R5)

R6. Each applicable Transmission Owner and applicable Generator Owner shall perform a Vegetation Inspection of 100% of its applicable transmission lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.) at least once per calendar

year and with no more than 18 calendar months between inspections on the same ROW[9] [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].

M6. Each applicable Transmission Owner and applicable Generator Owner has evidence that it conducted Vegetation Inspections of the transmission line ROW for all applicable lines at least once per calendar year but with no more than 18 calendar months between inspections on the same ROW. Examples of acceptable forms of evidence may include completed and dated work orders, dated invoices, or dated inspection records. (R6)

R7. Each applicable Transmission Owner and applicable Generator Owner shall complete 100% of its annual vegetation work plan of applicable lines to ensure no vegetation encroachments occur within the MVCD. Modifications to the work plan in response to changing conditions or to findings from vegetation inspections may be made (provided they do not allow encroachment of vegetation into the MVCD) and must be documented. The percent completed calculation is based on the number of units actually completed divided by the number of units in the final amended plan (measured in units of choice - circuit, pole line, line miles or kilometers, etc.). Examples of reasons for modification to annual plan may include [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*]:

- **7.1.** Change in expected growth rate/environmental factors
- **7.2.** Circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner[10]
- **7.3.** Rescheduling work between growing seasons
- **7.4.** Crew or contractor availability/Mutual assistance agreements
- **7.5.** Identified unanticipated high priority work
- **7.6.** Weather conditions/Accessibility
- **7.7.** Permitting delays
- **7.8.** Land ownership changes/Change in land use by the landowner
- **7.9.** Emerging technologies

M7. Each applicable Transmission Owner and applicable Generator Owner has evidence that it completed its annual vegetation work plan for its applicable lines. Examples of acceptable forms of evidence may include a copy of the completed annual work plan

[9] When the applicable Transmission Owner or applicable Generator Owner is prevented from performing a Vegetation Inspection within the timeframe in R6 due to a natural disaster, the TO or GO is granted a time extension that is equivalent to the duration of the time the TO or GO was prevented from performing the Vegetation Inspection.

[10] Circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner include but are not limited to natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, ice storms, floods, or major storms as defined either by the TO or GO or an applicable regulatory body.

(as finally modified), dated work orders, dated invoices, or dated inspection records. (R7)

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 applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirements R1, R2, R3, R5, R6 and R7, for three calendar years.
- The applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirement R4, Measure M4 for most recent 12 months of operator logs or most recent 3 months of voice recordings or transcripts of voice recordings, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- If an applicable Transmission Owner or applicable Generator Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time period specified above, whichever is longer.

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

Periodic Data Submittal: The applicable Transmission Owner and applicable Generator Owner will submit a quarterly report to its Regional Entity, or the Regional Entity's designee, identifying all Sustained Outages of applicable lines operated within their Rating and all Rated Electrical Operating Conditions as determined by the applicable Transmission Owner or applicable Generator Owner to have been caused by vegetation, except as excluded in footnote 2, and including as a minimum the following:

- The name of the circuit(s), the date, time and duration of the outage; the voltage of the circuit; a description of the cause of the outage; the category associated with the Sustained Outage; other pertinent comments; and any countermeasures taken by the applicable Transmission Owner or applicable Generator Owner.

  A Sustained Outage is to be categorized as one of the following:

- Category 1A — Grow-ins: Sustained Outages caused by vegetation growing into applicable lines, that are identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only), as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation, by vegetation inside and/or outside of the ROW;

- Category 1B — Grow-ins: Sustained Outages caused by vegetation growing into applicable lines, but are not identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lostor degraded are expected to result in instances of instability, Cascading, or uncontrolled separation, by vegetation inside and/or outside of the ROW;

- Category 2A — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines that are identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are epected to result in instances of instability, Cascading, or uncontrolled separation, from within the ROW;

- Category 2B — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines, but are not identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation, from within the ROW;

- Category 3 — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines from outside the ROW;

- Category 4A — Blowing together: Sustained Outages caused by vegetation and applicable lines that are identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation, blowing together from within the ROW;
- Category 4B — Blowing together: Sustained Outages caused by vegetation and applicable lines, but are not identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation, blowing together from within the ROW.

  The Regional Entity will report the outage information provided by applicable Transmission Owners and applicable Generator Owners, as per the above, quarterly to NERC, as well as any actions taken by the Regional Entity as a result of any of the reported Sustained Outages.

Violation Severity Levels (Table 1)

R #	Table 1: Violation Severity Levels (VSL)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation and encroachment into the MVCD as identified in FAC-003-4-Table 2 was observed in real time absent a Sustained Outage.	The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation and a vegetation-related Sustained Outage was caused by one of the following: • *A fall-in from inside the active transmission line ROW* • *Blowing together of applicable lines and*

				vegetation located inside the active transmission line ROW • *A grow-in*
R2.				•
R3.		The responsible entity has maintenance strategies or documented procedures or processes or specifications but has not accounted for the inter-relationships between vegetation growth rates, vegetation control methods, and inspection frequency, for the responsible entity's applicable lines. (Requirement R3, Part 3.2.)	The responsible entity has maintenance strategies or documented procedures or processes or specifications but has not accounted for the movement of transmission line conductors under their Rating and all Rated Electrical Operating Conditions, for the responsible entity's applicable lines. (Requirement R3, Part 3.1.)	The responsible entity does not have any maintenance strategies or documented procedures or processes or specifications used to prevent the encroachment of vegetation into the MVCD, for the responsible entity's applicable lines.
R4.			The responsible entity experienced a confirmed vegetation threat and notified the control center holding switching authority for that applicable line, but there was intentional delay in that notification.	The responsible entity experienced a confirmed vegetation threat and did not notify the control center holding switching authority for that applicable line.
R5.				The responsible entity did not take corrective action

				when it was constrained from performing planned vegetation work where an applicable line was put at potential risk.
R6.	The responsible entity failed to inspect 5% or less of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.)	The responsible entity failed to inspect more than 5% up to and including 10% of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.).	The responsible entity failed to inspect more than 10% up to and including 15% of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.).	The responsible entity failed to inspect more than 15% of its applicable lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.).
R7.	The responsible entity failed to complete 5% or less of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 5% and up to and including 10% of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 10% and up to and including 15% of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 15% of its annual vegetation work plan for its applicable lines (as finally modified).

D. Regional Variances

None.

E. Associated Documents

- FAC-003-4 Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	January 20, 2006	1. Added "Standard Development Roadmap." 2. Changed "60" to "Sixty" in section A, 5.2. 3. Added "Proposed Effective Date: April 7, 2006" to footer. 4. Added "Draft 3: November 17, 2005" to footer.	New
1	April 4, 2007	Regulatory Approval - Effective Date	New
2	November 3, 2011	Adopted by the NERC Board of Trustees	New
2	March 21, 2013	FERC Order issued approving FAC-003-2 (Order No. 777) FERC Order No. 777 was issued on March 21, 2013 directing NERC to "conduct or contract testing to obtain empirical data and submit a report to the Commission providing the results of the testing."[11]	Revisions
2	May 9, 2013	Board of Trustees adopted the modification of the VRF for Requirement R2 of FAC-003-2 by raising the VRF from "Medium" to "High."	Revisions
3	May 9, 2013	FAC-003-3 adopted by Board of Trustees	Revisions
3	September 19, 2013	A FERC order was issued on September 19, 2013, approving FAC-003-3. This standard became enforceable on July 1, 2014 for Transmission Owners. For Generator Owners, R3 became enforceable on January 1, 2015 and all other	Revisions

[11] *Revisions to Reliability Standard for Transmission Vegetation Management, Order No. 777,* 142 FERC ¶ 61,208 (2013)

		requirements (R1, R2, R4, R5, R6, and R7) became enforceable on January 1, 2016.	
3	November 22, 2013	Updated the VRF for R2 from “Medium” to “High” per a Final Rule issued by FERC	Revisions
3	July 30, 2014	Transferred the effective dates section from FAC-003-2 (for Transmission Owners) into FAC-003-3, per the FAC-003-3 implementation plan	Revisions
4	February 11, 2016	Adopted by Board of Trustees. Adjusted MVCD values in Table 2 for alternating current systems, consistent with findings reported in report filed on August 12, 2015 in Docket No. RM12-4-002 consistent with FERC’s directive in Order No. 777, and based on empirical testing results for flashover distances between conductors and vegetation.	Revisions
4	March 9, 2016	Corrected subpart 7.10 to M7, corrected value of .07 to .7	Errata
4	April 26, 2016	FERC Letter Order approving FAC-003-4. Docket No. RD16-4-000.	

FAC-003 — TABLE 2 — Minimum Vegetation Clearance Distances (MVCD)[12]

For **Alternating Current** Voltages (feet)

(AC) Nominal System Voltage (KV)[+]	(AC) Maximum System Voltage (kV)[13]	MVCD (feet) Over sea level up to 500 ft	MVCD feet Over 500 ft up to 1000 ft	MVCD feet Over 1000 ft up to 2000 ft	MVCD feet Over 2000 ft up to 3000 ft	MVCD feet Over 3000 ft up to 4000 ft	MVCD feet Over 4000 ft up to 5000 ft	MVCD feet Over 5000 ft up to 6000 ft	MVCD feet Over 6000 ft up to 7000 ft	MVCD feet Over 7000 ft up to 8000 ft	MVCD feet Over 8000 ft up to 9000 ft	MVCD feet Over 9000 ft up to 10000 ft	MVCD feet Over 10000 ft up to 11000 ft	MVCD feet Over 11000 ft up to 12000 ft	MVCD feet Over 12000 ft up to 13000 ft	MVCD feet Over 13000 ft up to 14000 ft	MVCD feet Over 14000 ft up to 15000 ft
765	800	11.6ft	11.7ft	11.9ft	12.1ft	12.2ft	12.4ft	12.6ft	12.8ft	13.0ft	13.1ft	13.3ft	13.5ft	13.7ft	13.9ft	14.1ft	14.3ft
500	550	7.0ft	7.1ft	7.2ft	7.4ft	7.5ft	7.6ft	7.8ft	7.9ft	8.1ft	8.2ft	8.3ft	8.5ft	8.6ft	8.8ft	8.9ft	9.1ft
345	362[14]	4.3ft	4.3ft	4.4ft	4.5ft	4.6ft	4.7ft	4.8ft	4.9ft	5.0ft	5.1ft	5.2ft	5.3ft	5.4ft	5.5ft	5.6ft	5.7ft
287	302	5.2ft	5.3ft	5.4ft	5.5ft	5.6ft	5.7ft	5.8ft	5.9ft	6.1ft	6.2ft	6.3ft	6.4ft	6.5ft	6.6ft	6.8ft	6.9ft
230	242	4.0ft	4.1ft	4.2ft	4.3ft	4.3ft	4.4ft	4.5ft	4.6ft	4.7ft	4.8ft	4.9ft	5.0ft	5.1ft	5.2ft	5.3ft	5.4ft
161*	169	2.7ft	2.7ft	2.8ft	2.9ft	2.9ft	3.0ft	3.0ft	3.1ft	3.2ft	3.3ft	3.3ft	3.4ft	3.5ft	3.6ft	3.7ft	3.8ft
138*	145	2.3ft	2.3ft	2.4ft	2.4ft	2.5ft	2.5ft	2.6ft	2.7ft	2.7ft	2.8ft	2.8ft	2.9ft	3.0ft	3.0ft	3.1ft	3.2ft
115*	121	1.9ft	1.9ft	1.9ft	2.0ft	2.0ft	2.1ft	2.1ft	2.2ft	2.2ft	2.3ft	2.3ft	2.4ft	2.5ft	2.5ft	2.6ft	2.7ft
88*	100	1.5ft	1.5ft	1.6ft	1.6ft	1.7ft	1.7ft	1.8ft	1.8ft	1.8ft	1.9ft	1.9ft	2.0ft	2.0ft	2.1ft	2.2ft	2.2ft
69*	72	1.1ft	1.1ft	1.1ft	1.2ft	1.2ft	1.2ft	1.2ft	1.3ft	1.3ft	1.3ft	1.4ft	1.4ft	1.4ft	1.5ft	1.6ft	1.6ft

* Such lines are applicable to this standard only if PC has determined such per FAC-014 (refer to the Applicability Section above)

[+] *Table 2 – Table of MVCD values at a 1.0 gap factor (in U.S. customary units), which is located in the EPRI report filed with FERC on August 12, 2015. (The 14000-15000 foot values were subsequently provided by EPRI in an updated Table 2 on December 1, 2015, filed with the FAC-003-4 Petition at FERC)*

[12] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

[13] Where applicable lines are operated at nominal voltages other than those listed, the applicable Transmission Owner or applicable Generator Owner should use the maximum system voltage to determine the appropriate clearance for that line.

[14] The change in transient overvoltage factors in the calculations are the driver in the decrease in MVCDs for voltages of 345 kV and above. Refer to pp.29-31 in the Supplemental Materials for additional information.

TABLE 2 (CONT) — Minimum Vegetation Clearance Distances (MVCD)[15]

For **Alternating Current** Voltages (meters)

(AC) Nominal System Voltage (KV)+	(AC) Maximum System Voltage (kV)[16]	MVCD meters Over sea level up to 153 m	MVCD meters Over 153m up to 305m	MVCD meters Over 305m up to 610m	MVCD meters Over 610m up to 915m	MVCD meters Over 915m up to 1220m	MVCD meters Over 1220m up to 1524m	MVCD meters Over 1524m up to 1829m	MVCD meters Over 1829m up to 2134m	MVCD meters Over 2134m up to 2439m	MVCD meters Over 2439m up to 2744m	MVCD meters Over 2744m up to 3048m	MVCD meters Over 3048m up to 3353m	MVCD meters Over 3353m up to 3657m	MVCD meters Over 3657m up to 3962m	MVCD meters Over 3962 m up to 4268 m	MVCD meters Over 4268m up to 4572m
765	800	3.6m	3.6m	3.6m	3.7m	3.7m	3.8m	3.8m	3.9m	4.0m	4.0m	4.1m	4.1m	4.2m	4.2m	4.3m	4.4m
500	550	2.1m	2.2m	2.2m	2.3m	2.3m	2.3m	2.4m	2.4m	2.5m	2..5m	2.5m	2.6m	2.6m	2.7m	2.7m	2.7m
345	362[17]	1.3m	1.3m	1.3m	1.4m	1.4m	1.4m	1.5m	1.5m	1.5m	1.6m	1.6m	1.6m	1.6m	1.7m	1.7m	1.8m
287	302	1.6m	1.6m	1.7m	1.7m	1.7m	1.7m	1.8m	1.8m	1.9m	1.9m	1.9m	2.0m	2.0m	2.0m	2.1m	2.1m
230	242	1.2m	1.3m	1.3m	1.3m	1.3m	1.3m	1.4m	1.4m	1.4m	1.5m	1.5m	1.5m	1.6m	1.6m	1.6m	1.6m
161*	169	0.8m	0.8m	0.9m	0.9m	0.9m	0.9m	0.9m	1.0m	1.0m	1.0m	1.0m	1.0m	1.1m	1.1m	1.1m	1.1m
138*	145	0.7m	0.7m	0.7m	0.7m	0.7m	0.7m	0.8m	0.8m	0.8m	0.9m	0.9m	0.9m	0.9m	0.9m	1.0m	1.0m
115*	121	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.7m	0.7m	0.7m	0.7m	0.7m	0.8m	0.8m	0.8m	0.8m
88*	100	0.4m	0.4m	0.5m	0.5m	0.5m	0.5m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.7m	0.7m
69*	72	0.3m	0.3m	0.3m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.5m	0.5m	0.5m

* Such lines are applicable to this standard only if PC has determined such per FAC-014 (refer to the Applicability Section above)

+ *Table 2 – Table of MVCD values at a 1.0 gap factor (in U.S. customary units), which is located in the EPRI report filed with FERC on August 12, 2015. (The 14000-15000 foot values were subsequently provided by EPRI in an updated Table 2 on December 1, 2015, filed with the FAC-003-4 Petition at FERC)*

[15] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

[16] Where applicable lines are operated at nominal voltages other than those listed, the applicable Transmission Owner or applicable Generator Owner should use the maximum system voltage to determine the appropriate clearance for that line.

[17] The change in transient overvoltage factors in the calculations are the driver in the decrease in MVCDs for voltages of 345 kV and above. Refer to pp.29-31 in the supplemental materials for additional information.

TABLE 2 (CONT) — Minimum Vegetation Clearance Distances (MVCD)[18]

For **Direct Current** Voltages feet (meters)

(DC) Nominal Pole to Ground Voltage (kV)	MVCD meters Over sea level up to 500 ft (Over sea level up to 152.4 m)	MVCD meters Over 500 ft up to 1000 ft (Over 152.4 m up to 304.8 m	MVCD meters Over 1000 ft up to 2000 ft (Over 304.8 m up to 609.6m)	MVCD meters Over 2000 ft up to 3000 ft (Over 609.6m up to 914.4m	MVCD meters Over 3000 ft up to 4000 ft (Over 914.4m up to 1219.2m	MVCD meters Over 4000 ft up to 5000 ft (Over 1219.2m up to 1524m	MVCD meters Over 5000 ft up to 6000 ft (Over 1524 m up to 1828.8 m)	MVCD meters Over 6000 ft up to 7000 ft (Over 1828.8m up to 2133.6m)	MVCD meters Over 7000 ft up to 8000 ft (Over 2133.6m up to 2438.4m)	MVCD meters Over 8000 ft up to 9000 ft (Over 2438.4m up to 2743.2m)	MVCD meters Over 9000 ft up to 10000 ft (Over 2743.2m up to 3048m)	MVCD meters Over 10000 ft up to 11000 ft (Over 3048m up to 3352.8m)
±750	14.12ft (4.30m)	14.31ft (4.36m)	14.70ft (4.48m)	15.07ft (4.59m)	15.45ft (4.71m)	15.82ft (4.82m)	16.2ft (4.94m)	16.55ft (5.04m)	16.91ft (5.15m)	17.27ft (5.26m)	17.62ft (5.37m)	17.97ft (5.48m)
±600	10.23ft (3.12m)	10.39ft (3.17m)	10.74ft (3.26m)	11.04ft (3.36m)	11.35ft (3.46m)	11.66ft (3.55m)	11.98ft (3.65m)	12.3ft (3.75m)	12.62ft (3.85m)	12.92ft (3.94m)	13.24ft (4.04m)	13.54ft (4.13m)
±500	8.03ft (2.45m)	8.16ft (2.49m)	8.44ft (2.57m)	8.71ft (2.65m)	8.99ft (2.74m)	9.25ft (2.82m)	9.55ft (2.91m)	9.82ft (2.99m)	10.1ft (3.08m)	10.38ft (3.16m)	10.65ft (3.25m)	10.92ft (3.33m)
±400	6.07ft (1.85m)	6.18ft (1.88m)	6.41ft (1.95m)	6.63ft (2.02m)	6.86ft (2.09m)	7.09ft (2.16m)	7.33ft (2.23m)	7.56ft (2.30m)	7.80ft (2.38m)	8.03ft (2.45m)	8.27ft (2.52m)	8.51ft (2.59m)
±250	3.50ft (1.07m)	3.57ft (1.09m)	3.72ft (1.13m)	3.87ft (1.18m)	4.02ft (1.23m)	4.18ft (1.27m)	4.34ft (1.32m)	4.5ft (1.37m)	4.66ft (1.42m)	4.83ft (1.47m)	5.00ft (1.52m)	5.17ft (1.58m)

[18] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

Guideline and Technical Basis

Effective dates:

The Compliance section is standard language used in most NERC standards to cover the general effective date and covers the vast majority of situations. A special case covers effective dates for (1) lines initially becoming subject to the Standard, (2) lines changing in applicability within the standard.

The special case is needed because the Planning Coordinators may designate lines below 200 kV, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation, in a future Planning Year (PY). For example, studies by the Planning Coordinator in 2015 may identify a line to have that designation beginning in PY 2025, ten years after the planning study is performed. It is not intended for the Standard to be immediately applicable to, or in effect for, that line until that future PY begins. The effective date provision for such lines ensures that the line will become subject to the standard on January 1 of the PY specified with an allowance of at least 12 months for the applicable Transmission Owner or applicable Generator Owner to make the necessary preparations to achieve compliance on that line. A line operating below 200kV designated by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation may be removed from that designation due to system improvements, changes in generation, changes in loads or changes in studies and analysis of the network.

Date that Planning Study is completed	PY the line will become an identified element	Date 1	Date 2	Effective Date The later of Date 1 or Date 2
05/15/2011	2012	05/15/2012	01/01/2012	05/15/2012
05/15/2011	2013	05/15/2012	01/01/2013	01/01/2013
05/15/2011	2014	05/15/2012	01/01/2014	01/01/2014
05/15/2011	2021	05/15/2012	01/01/2021	01/01/2021

Defined Terms:

Explanation for revising the definition of ROW:
The current NERC glossary definition of Right of Way has been modified to include Generator Owners and to address the matter set forth in Paragraph 734 of FERC Order 693. The Order pointed out that Transmission Owners may in some cases own more property or rights than are needed to reliably operate transmission lines. This definition represents a slight but significant

departure from the strict legal definition of "right of way" in that this definition is based on engineering and construction considerations that establish the width of a corridor from a technical basis. The pre-2007 maintenance records are included in the current definition to allow the use of such vegetation widths if there were no engineering or construction standards that referenced the width of right of way to be maintained for vegetation on a particular line but the evidence exists in maintenance records for a width that was in fact maintained prior to this standard becoming mandatory. Such widths may be the only information available for lines that had limited or no vegetation easement rights and were typically maintained primarily to ensure public safety. This standard does not require additional easement rights to be purchased to satisfy a minimum right of way width that did not exist prior to this standard becoming mandatory.

Explanation for revising the definition of Vegetation Inspection:
The current glossary definition of this NERC term was modified to include Generator Owners and to allow both maintenance inspections and vegetation inspections to be performed concurrently. This allows potential efficiencies, especially for those lines with minimal vegetation and/or slow vegetation growth rates.

Explanation of the derivation of the MVCD:
The MVCD is a calculated minimum distance that is derived from the Gallet equation. This is a method of calculating a flash over distance that has been used in the design of high voltage transmission lines. Keeping vegetation away from high voltage conductors by this distance will prevent voltage flash-over to the vegetation. See the explanatory text below for Requirement R3 and associated Figure 1. Table 2 of the standard provides MVCD values for various voltages and altitudes. The table is based on empirical testing data from EPRI as requested by FERC in Order No. 777.

Project 2010-07.1 Adjusted MVCDs per EPRI Testing:
In Order No. 777, FERC directed NERC to undertake testing to gather empirical data validating the appropriate gap factor used in the Gallet equation to calculate MVCDs, specifically the gap factor for the flash-over distances between conductors and vegetation. See, Order No. 777, at P 60. NERC engaged industry through a collaborative research project and contracted EPRI to complete the scope of work. In January 2014, NERC formed an advisory group to assist with developing the scope of work for the project. This team provided subject matter expertise for developing the test plan, monitoring testing, and vetting the analysis and conclusions to be submitted in a final report. The advisory team was comprised of NERC staff, arborists, and industry members with wide-ranging expertise in transmission engineering, insulation coordination, and vegetation management. The testing project commenced in April 2014 and continued through October 2014 with the final set of testing completed in May 2015. Based on these testing results conducted by EPRI, and consistent with the report filed in FERC Docket No. RM12-4-000, the gap factor used in the Gallet equation required adjustment from 1.3 to 1.0. This resulted in increased MVCD values for all alternating current system voltages identified. The adjusted MVCD values, reflecting the 1.0 gap factor, are included in Table 2 of version 4 of FAC-003.

The air gap testing completed by EPRI per FERC Order No. 777 established that trees with large spreading canopies growing directly below energized high voltage conductors create the greatest likelihood of an air gap flash over incident and was a key driver in changing the gap factor to a more conservative value of 1.0 in version 4 of this standard.

Requirements R1 and R2:
R1 and R2 are performance-based requirements. The reliability objective or outcome to be achieved is the management of vegetation such that there are no vegetation encroachments within a minimum distance of transmission lines. Content-wise, R1 and R2 are the same requirements; however, they apply to different Facilities. Both R1 and R2 require each applicable Transmission Owner or applicable Generator Owner to manage vegetation to prevent encroachment within the MVCD of transmission lines. R1 is applicable to lines that are identified as an element by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation. R2 is applicable to all other lines that are not identified as an element by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation.

The separation of applicability (between R1 and R2) recognizes that inadequate vegetation management for an applicable line has been identified as an element by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lostor degraded are expected to result in instances of instability, Cascading, or uncontrolled separation is a greater risk to the interconnected electric transmission system than applicable lines that have not been identified as such. Applicable lines that have not been identified as such do require effective vegetation management, but these lines are comparatively less operationally significant.

Requirements R1 and R2 state that if inadequate vegetation management allows vegetation to encroach within the MVCD distance as shown in Table 2, it is a violation of the standard. Table 2 distances are the minimum clearances that will prevent spark-over based on the Gallet equations. These requirements assume that transmission lines and their conductors are operating within their Rating. If a line conductor is intentionally or inadvertently operated beyond its Rating and Rated Electrical Operating Condition (potentially in violation of other standards), the occurrence of a clearance encroachment may occur solely due to that condition. For example, emergency actions taken by an applicable Transmission Owner or applicable Generator Owner or Reliability Coordinator to protect an Interconnection may cause excessive sagging and an outage. Another example would be ice loading beyond the line's Rating and Rated Electrical Operating Condition. Such vegetation-related encroachments and outages are not violations of this standard.

Evidence of failures to adequately manage vegetation include real-time observation of a vegetation encroachment into the MVCD (absent a Sustained Outage), or a vegetation-related encroachment resulting in a Sustained Outage due to a fall-in from inside the ROW, or a vegetation-related encroachment resulting in a Sustained Outage due to the blowing together of the lines and vegetation located inside the ROW, or a vegetation-related encroachment resulting in a Sustained Outage due to a grow-in. Faults which do not cause a Sustained outage and which are confirmed to have been caused by vegetation encroachment within the MVCD are considered the equivalent of a Real-time observation for violation severity levels.

With this approach, the VSLs for R1 and R2 are structured such that they directly correlate to the severity of a failure of an applicable Transmission Owner or applicable Generator Owner to manage vegetation and to the corresponding performance level of the Transmission Owner's vegetation program's ability to meet the objective of "preventing the risk of those vegetation related outages that could lead to Cascading." Thus violation severity increases with an applicable Transmission Owner's or applicable Generator Owner's inability to meet this goal and its potential of leading to a Cascading event. The additional benefits of such a combination are that it simplifies the standard and clearly defines performance for compliance. A performance-based requirement of this nature will promote high quality, cost effective vegetation management programs that will deliver the overall end result of improved reliability to the system.

Multiple Sustained Outages on an individual line can be caused by the same vegetation. For example initial investigations and corrective actions may not identify and remove the actual outage cause then another outage occurs after the line is re-energized and previous high conductor temperatures return. Such events are considered to be a single vegetation-related Sustained Outage under the standard where the Sustained Outages occur within a 24 hour period.

If the applicable Transmission Owner or applicable Generator Owner has applicable lines operated at nominal voltage levels not listed in Table 2, then the applicable TO or applicable GO should use the next largest clearance distance based on the next highest nominal voltage in the table to determine an acceptable distance.

Requirement R3:
R3 is a competency based requirement concerned with the maintenance strategies, procedures, processes, or specifications, an applicable Transmission Owner or applicable Generator Owner uses for vegetation management.

An adequate transmission vegetation management program formally establishes the approach the applicable Transmission Owner or applicable Generator Owner uses to plan and perform vegetation work to prevent transmission Sustained Outages and minimize risk to the transmission system. The approach provides the basis for evaluating the intent, allocation of appropriate resources, and the competency of the applicable Transmission Owner or applicable Generator Owner in managing vegetation. There are many acceptable approaches to manage

vegetation and avoid Sustained Outages. However, the applicable Transmission Owner or applicable Generator Owner must be able to show the documentation of its approach and how it conducts work to maintain clearances.

An example of one approach commonly used by industry is ANSI Standard A300, part 7. However, regardless of the approach a utility uses to manage vegetation, any approach an applicable Transmission Owner or applicable Generator Owner chooses to use will generally contain the following elements:

1. *the maintenance strategy used (such as minimum vegetation-to-conductor distance or maximum vegetation height) to ensure that MVCD clearances are never violated*
2. *the work methods that the applicable Transmission Owner or applicable Generator Owner uses to control vegetation*
3. *a stated Vegetation Inspection frequency*
4. *an annual work plan*

The conductor's position in space at any point in time is continuously changing in reaction to a number of different loading variables. Changes in vertical and horizontal conductor positioning are the result of thermal and physical loads applied to the line. Thermal loading is a function of line current and the combination of numerous variables influencing ambient heat dissipation including wind velocity/direction, ambient air temperature and precipitation. Physical loading applied to the conductor affects sag and sway by combining physical factors such as ice and wind loading. The movement of the transmission line conductor and the MVCD is illustrated in Figure 1 below.

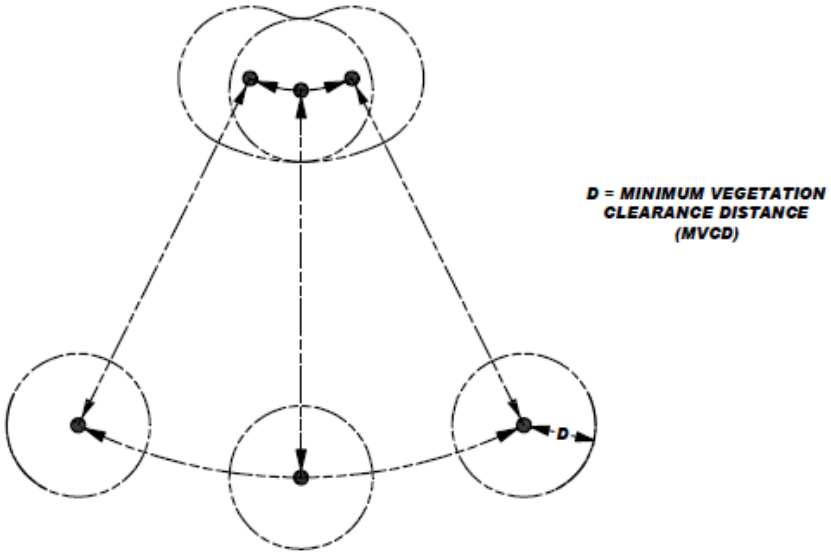


Figure 1

A cross-section view of a single conductor at a given point along the span is shown with six possible conductor positions due to movement resulting from thermal and mechanical loading.

Requirement R4:
R4 is a risk-based requirement. It focuses on preventative actions to be taken by the applicable Transmission Owner or applicable Generator Owner for the mitigation of Fault risk when a vegetation threat is confirmed. R4 involves the notification of potentially threatening vegetation conditions, without any intentional delay, to the control center holding switching authority for that specific transmission line. Examples of acceptable unintentional delays may include communication system problems (for example, cellular service or two-way radio disabled), crews located in remote field locations with no communication access, delays due to severe weather, etc.

Confirmation is key that a threat actually exists due to vegetation. This confirmation could be in the form of an applicable Transmission Owner or applicable Generator Owner employee who personally identifies such a threat in the field. Confirmation could also be made by sending out an employee to evaluate a situation reported by a landowner.

Vegetation-related conditions that warrant a response include vegetation that is near or encroaching into the MVCD (a grow-in issue) or vegetation that could fall into the transmission conductor (a fall-in issue). A knowledgeable verification of the risk would include an assessment of the possible sag or movement of the conductor while operating between no-load conditions and its rating.

The applicable Transmission Owner or applicable Generator Owner has the responsibility to ensure the proper communication between field personnel and the control center to allow the control center to take the appropriate action until or as the vegetation threat is relieved. Appropriate actions may include a temporary reduction in the line loading, switching the line out of service, or other preparatory actions in recognition of the increased risk of outage on that circuit. The notification of the threat should be communicated in terms of minutes or hours as opposed to a longer time frame for corrective action plans (see R5).

All potential grow-in or fall-in vegetation-related conditions will not necessarily cause a Fault at any moment. For example, some applicable Transmission Owners or applicable Generator Owners may have a danger tree identification program that identifies trees for removal with the potential to fall near the line. These trees would not require notification to the control center unless they pose an immediate fall-in threat.

Requirement R5:
R5 is a risk-based requirement. It focuses upon preventative actions to be taken by the applicable Transmission Owner or applicable Generator Owner for the mitigation of Sustained

Outage risk when temporarily constrained from performing vegetation maintenance. The intent of this requirement is to deal with situations that prevent the applicable Transmission Owner or applicable Generator Owner from performing planned vegetation management work and, as a result, have the potential to put the transmission line at risk. Constraints to performing vegetation maintenance work as planned could result from legal injunctions filed by property owners, the discovery of easement stipulations which limit the applicable Transmission Owner's or applicable Generator Owner's rights, or other circumstances.

This requirement is not intended to address situations where the transmission line is not at potential risk and the work event can be rescheduled or re-planned using an alternate work methodology. For example, a land owner may prevent the planned use of herbicides to control incompatible vegetation outside of the MVCD, but agree to the use of mechanical clearing. In this case the applicable Transmission Owner or applicable Generator Owner is not under any immediate time constraint for achieving the management objective, can easily reschedule work using an alternate approach, and therefore does not need to take interim corrective action.

However, in situations where transmission line reliability is potentially at risk due to a constraint, the applicable Transmission Owner or applicable Generator Owner is required to take an interim corrective action to mitigate the potential risk to the transmission line. A wide range of actions can be taken to address various situations. General considerations include:

- Identifying locations where the applicable Transmission Owner or applicable Generator Owner is constrained from performing planned vegetation maintenance work which potentially leaves the transmission line at risk.
- Developing the specific action to mitigate any potential risk associated with not performing the vegetation maintenance work as planned.
- Documenting and tracking the specific action taken for the location.
- In developing the specific action to mitigate the potential risk to the transmission line the applicable Transmission Owner or applicable Generator Owner could consider location specific measures such as modifying the inspection and/or maintenance intervals. Where a legal constraint would not allow any vegetation work, the interim corrective action could include limiting the loading on the transmission line.
- The applicable Transmission Owner or applicable Generator Owner should document and track the specific corrective action taken at each location. This location may be indicated as one span, one tree or a combination of spans on one property where the constraint is considered to be temporary.

Requirement R6:
R6 is a risk-based requirement. This requirement sets a minimum time period for completing Vegetation Inspections. The provision that Vegetation Inspections can be performed in conjunction with general line inspections facilitates a Transmission Owner's ability to meet this requirement. However, the applicable Transmission Owner or applicable Generator Owner may determine that more frequent vegetation specific inspections are needed to maintain

reliability levels, based on factors such as anticipated growth rates of the local vegetation, length of the local growing season, limited ROW width, and local rainfall. Therefore it is expected that some transmission lines may be designated with a higher frequency of inspections.

The VSLs for Requirement R6 have levels ranked by the failure to inspect a percentage of the applicable lines to be inspected. To calculate the appropriate VSL the applicable Transmission Owner or applicable Generator Owner may choose units such as: circuit, pole line, line miles or kilometers, etc.

For example, when an applicable Transmission Owner or applicable Generator Owner operates 2,000 miles of applicable transmission lines this applicable Transmission Owner or applicable Generator Owner will be responsible for inspecting all the 2,000 miles of lines at least once during the calendar year. If one of the included lines was 100 miles long, and if it was not inspected during the year, then the amount failed to inspect would be 100/2000 = 0.05 or 5%. The "Low VSL" for R6 would apply in this example.

Requirement R7:
R7 is a risk-based requirement. The applicable Transmission Owner or applicable Generator Owner is required to complete its annual work plan for vegetation management to accomplish the purpose of this standard. Modifications to the work plan in response to changing conditions or to findings from vegetation inspections may be made and documented provided they do not put the transmission system at risk. The annual work plan requirement is not intended to necessarily require a "span-by-span", or even a "line-by-line" detailed description of all work to be performed. It is only intended to require that the applicable Transmission Owner or applicable Generator Owner provide evidence of annual planning and execution of a vegetation management maintenance approach which successfully prevents encroachment of vegetation into the MVCD.

When an applicable Transmission Owner or applicable Generator Owner identifies 1,000 miles of applicable transmission lines to be completed in the applicable Transmission Owner's or applicable Generator Owner's annual plan, the applicable Transmission Owner or applicable Generator Owner will be responsible completing those identified miles. If an applicable Transmission Owner or applicable Generator Owner makes a modification to the annual plan that does not put the transmission system at risk of an encroachment the annual plan may be modified. If 100 miles of the annual plan is deferred until next year the calculation to determine what percentage was completed for the current year would be: 1000 – 100 (deferred miles) = 900 modified annual plan, or 900 / 900 = 100% completed annual miles. If an applicable Transmission Owner or applicable Generator Owner only completed 875 of the total 1000 miles with no acceptable documentation for modification of the annual plan the calculation for failure to complete the annual plan would be: 1000 – 875 = 125 miles failed to complete then, 125 miles (not completed) / 1000 total annual plan miles = 12.5% failed to complete.

The ability to modify the work plan allows the applicable Transmission Owner or applicable Generator Owner to change priorities or treatment methodologies during the year as conditions or situations dictate. For example recent line inspections may identify unanticipated high priority work, weather conditions (drought) could make herbicide application ineffective during the plan year, or a major storm could require redirecting local resources away from planned maintenance. This situation may also include complying with mutual assistance agreements by moving resources off the applicable Transmission Owner's or applicable Generator Owner's system to work on another system. Any of these examples could result in acceptable deferrals or additions to the annual work plan provided that they do not put the transmission system at risk of a vegetation encroachment.
In general, the vegetation management maintenance approach should use the full extent of the applicable Transmission Owner's or applicable Generator Owner's easement, fee simple and other legal rights allowed. A comprehensive approach that exercises the full extent of legal rights on the ROW is superior to incremental management because in the long term it reduces the overall potential for encroachments, and it ensures that future planned work and future planned inspection cycles are sufficient.

When developing the annual work plan the applicable Transmission Owner or applicable Generator Owner should allow time for procedural requirements to obtain permits to work on federal, state, provincial, public, tribal lands. In some cases the lead time for obtaining permits may necessitate preparing work plans more than a year prior to work start dates. Applicable Transmission Owners or applicable Generator Owners may also need to consider those special landowner requirements as documented in easement instruments.

This requirement sets the expectation that the work identified in the annual work plan will be completed as planned. Therefore, deferrals or relevant changes to the annual plan shall be documented. Depending on the planning and documentation format used by the applicable Transmission Owner or applicable Generator Owner, evidence of successful annual work plan execution could consist of signed-off work orders, signed contracts, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, or paid invoices. Other evidence may include photographs, and walk-through reports.

Notes:

The SDT determined that the use of IEEE 516-2003 in version 1 of FAC-003 was a misapplication. The SDT consulted specialists who advised that the Gallet equation would be a technically justified method. The explanation of why the Gallet approach is more appropriate is explained in the paragraphs below.

The drafting team sought a method of establishing minimum clearance distances that uses realistic weather conditions and realistic maximum transient over-voltages factors for in-service transmission lines.

The SDT considered several factors when looking at changes to the minimum vegetation to conductor distances in FAC-003-1:

- avoid the problem associated with referring to tables in another standard (IEEE-516-2003)
- transmission lines operate in non-laboratory environments (wet conditions)
- transient over-voltage factors are lower for in-service transmission lines than for inadvertently re-energized transmission lines with trapped charges.

FAC-003-1 used the minimum air insulation distance (MAID) without tools formula provided in IEEE 516-2003 to determine the minimum distance between a transmission line conductor and vegetation. The equations and methods provided in IEEE 516 were developed by an IEEE Task Force in 1968 from test data provided by thirteen independent laboratories. The distances provided in IEEE 516 Tables 5 and 7 are based on the withstand voltage of a dry rod-rod air gap, or in other words, dry laboratory conditions. Consequently, the validity of using these distances in an outside environment application has been questioned.

FAC-003-1 allowed Transmission Owners to use either Table 5 or Table 7 to establish the minimum clearance distances. Table 7 could be used if the Transmission Owner knew the maximum transient over-voltage factor for its system. Otherwise, Table 5 would have to be used. Table 5 represented minimum air insulation distances under the worst possible case for transient over-voltage factors. These worst case transient over-voltage factors were as follows: 3.5 for voltages up to 362 kV phase to phase; 3.0 for 500 - 550 kV phase to phase; and 2.5 for 765 to 800 kV phase to phase. These worst case over-voltage factors were also a cause for concern in this particular application of the distances.

In general, the worst case transient over-voltages occur on a transmission line that is inadvertently re-energized immediately after the line is de-energized and a trapped charge is still present. The intent of FAC-003 is to keep a transmission line that is in service from becoming de-energized (i.e. tripped out) due to spark-over from the line conductor to nearby vegetation. Thus, the worst case transient overvoltage assumptions are not appropriate for this application. Rather, the appropriate over voltage values are those that occur only while the line is energized.

Typical values of transient over-voltages of in-service lines are not readily available in the literature because they are negligible compared with the maximums. A conservative value for the maximum transient over-voltage that can occur anywhere along the length of an in-service ac line was approximately 2.0 per unit. This value was a conservative estimate of the transient over-voltage that is created at the point of application (e.g. a substation) by switching a capacitor bank without pre-insertion devices (e.g. closing resistors). At voltage levels where capacitor banks are not very common (e.g. Maximum System Voltage of 362 kV), the maximum transient over-voltage of an in-service ac line are created by fault initiation on adjacent ac lines and shunt reactor bank switching. These transient voltages are usually 1.5 per unit or less.

Even though these transient over-voltages will not be experienced at locations remote from the bus at which they are created, in order to be conservative, it is assumed that all nearby ac lines

are subjected to this same level of over-voltage. Thus, a maximum transient over-voltage factor of 2.0 per unit for transmission lines operated at 302 kV and below was considered to be a realistic maximum in this application. Likewise, for ac transmission lines operated at Maximum System Voltages of 362 kV and above a transient over-voltage factor of 1.4 per unit was considered a realistic maximum.

The Gallet equations are an accepted method for insulation coordination in tower design. These equations are used for computing the required strike distances for proper transmission line insulation coordination. They were developed for both wet and dry applications and can be used with any value of transient over-voltage factor. The Gallet equation also can take into account various air gap geometries. This approach was used to design the first 500 kV and 765 kV lines in North America.

If one compares the MAID using the IEEE 516-2003 Table 7 (table D.5 for English values) with the critical spark-over distances computed using the Gallet wet equations, for each of the nominal voltage classes and identical transient over-voltage factors, the Gallet equations yield a more conservative (larger) minimum distance value.

Distances calculated from either the IEEE 516 (dry) formulas or the Gallet "wet" formulas are not vastly different when the same transient overvoltage factors are used; the "wet" equations will consistently produce slightly larger distances than the IEEE 516 equations when the same transient overvoltage is used. While the IEEE 516 equations were only developed for dry conditions the Gallet equations have provisions to calculate spark-over distances for both wet and dry conditions.

Since no empirical data for spark over distances to live vegetation existed at the time version 3 was developed, the SDT chose a proven method that has been used in other EHV applications. The Gallet equations relevance to wet conditions and the selection of a Transient Overvoltage Factor that is consistent with the absence of trapped charges on an in-service transmission line make this methodology a better choice.

The following table is an example of the comparison of distances derived from IEEE 516 and the Gallet equations.

Comparison of spark-over distances computed using Gallet wet equations vs.

IEEE 516-2003 MAID distances

(AC) Nom System Voltage (kV)	(AC) Max System Voltage (kV)	Transient Over-voltage Factor (T)	Clearance (ft.) Gallet (wet) @ Alt. 3000 feet	Table 7 (Table D.5 for feet) IEEE 516-2003 MAID (ft) @ Alt. 3000 feet

765	800	2.0	14.36	13.95
500	550	2.4	11.0	10.07
345	362	3.0	8.55	7.47
230	242	3.0	5.28	4.2
115	121	3.0	2.46	2.1

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 Applicability (section 4.2.4):
The areas excluded in 4.2.4 were excluded based on comments from industry for reasons summarized as follows:

1) There is a very low risk from vegetation in this area. Based on an informal survey, no TOs reported such an event.
2) Substations, switchyards, and stations have many inspection and maintenance activities that are necessary for reliability. Those existing process manage the threat. As such, the formal steps in this standard are not well suited for this environment.
3) Specifically addressing the areas where the standard does and does not apply makes the standard clearer.

Rationale for Applicability (section 4.3):
Within the text of NERC Reliability Standard FAC-003-3, “transmission line(s)” and “applicable line(s)” can also refer to the generation Facilities as referenced in 4.3 and its subsections.

Rationale for R1:
Lines with the highest significance to reliability are covered in R1; all other lines are covered in R2.

Rationale for the types of failure to manage vegetation which are listed in order of increasing degrees of severity in non-compliant performance as it relates to a failure of an applicable Transmission Owner's or applicable Generator Owner’s vegetation maintenance program:

1. This management failure is found by routine inspection or Fault event investigation, and is normally symptomatic of unusual conditions in an otherwise sound program.
2. This management failure occurs when the height and location of a side tree within the ROW is not adequately addressed by the program.
3. This management failure occurs when side growth is not adequately addressed and may be indicative of an unsound program.
4. This management failure is usually indicative of a program that is not addressing the most fundamental dynamic of vegetation management, (i.e. a grow-in under the line). If this type of failure is pervasive on multiple lines, it provides a mechanism for a Cascade.

Rationale for R3:
The documentation provides a basis for evaluating the competency of the applicable Transmission Owner’s or applicable Generator Owner’s vegetation program. There may be many acceptable approaches to maintain clearances. Any approach must demonstrate that the

applicable Transmission Owner or applicable Generator Owner avoids vegetation-to-wire conflicts under all Ratings and all Rated Electrical Operating Conditions.

Rationale for R4:

This is to ensure expeditious communication between the applicable Transmission Owner or applicable Generator Owner and the control center when a critical situation is confirmed.

Rationale for R5:

Legal actions and other events may occur which result in constraints that prevent the applicable Transmission Owner or applicable Generator Owner from performing planned vegetation maintenance work.

In cases where the transmission line is put at potential risk due to constraints, the intent is for the applicable Transmission Owner and applicable Generator Owner to put interim measures in place, rather than do nothing.

The corrective action process is not intended to address situations where a planned work methodology cannot be performed but an alternate work methodology can be used.

Rationale for R6:

Inspections are used by applicable Transmission Owners and applicable Generator Owners to assess the condition of the entire ROW. The information from the assessment can be used to determine risk, determine future work and evaluate recently-completed work. This requirement sets a minimum Vegetation Inspection frequency of once per calendar year but with no more than 18 months between inspections on the same ROW. Based upon average growth rates across North America and on common utility practice, this minimum frequency is reasonable. Transmission Owners should consider local and environmental factors that could warrant more frequent inspections.

Rationale for R7:

This requirement sets the expectation that the work identified in the annual work plan will be completed as planned. It allows modifications to the planned work for changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors, provided that those modifications do not put the transmission system at risk of a vegetation encroachment.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** Transmission Vegetation Management

2. **Number:** FAC-003-54

3. **Purpose:** To maintain a reliable electric transmission system by using a defense-in-depth strategy to manage vegetation located on transmission rights of way (ROW) and minimize encroachments from vegetation located adjacent to the ROW, thus preventing the risk of those vegetation-related outages that could lead to Cascading.

4. **Applicability:**

4.1. Functional Entities:

4.1.1. Applicable Transmission Owners

4.1.1.1. Transmission Owners that own Transmission Facilities defined in 4.2.

4.1.2. Applicable Generator Owners

4.1.2.1. Generator Owners that own generation Facilities defined in 4.3.

4.2. Transmission Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[1], state, provincial, public, private, or tribal entities:

4.2.1. Each overhead transmission line operated at 200kV or higher.

4.2.2. Each overhead transmission line operated below 200kV, identified by the Planning Coordinator or Transmission Planner, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as a Facility that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation.~~identified as an element of an IROL under NERC Standard FAC-014 by the Planning Coordinator.~~

4.2.3. Each overhead transmission line operated below 200 kV identified as an element of a Major Western Electricity Coordinating Council (WECC) Transfer Path in the Bulk Electric System by WECC.

4.2.4. Each overhead transmission line identified above (4.2.1. through 4.2.3.) located outside the fenced area of the switchyard, station or substation and any portion of the span of the transmission line that is crossing the substation fence.

[1] EPAct 2005 section 1211c: *"Access approvals by Federal agencies."*

4.3. Generation Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[2], state, provincial, public, private, or tribal entities:

4.3.1. Overhead transmission lines that (1) extend greater than one mile or 1.609 kilometers beyond the fenced area of the generating station switchyard to the point of interconnection with a Transmission Owner's Facility or (2) do not have a clear line of sight[3] from the generating station switchyard fence to the point of interconnection with a Transmission Owner's Facility and are:

4.3.1.1. Operated at 200kV or higher; or

4.3.1.2. Operated below 200kV and are identified by the Planning Coordinator or Transmission Planner, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as a Facility that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation.~~identified as an element of an IROL under NERC Standard FAC-014 by the Planning Coordinator~~; or

4.3.1.3. Operated below 200 kV identified as an element of a Major WECC Transfer Path in the Bulk Electric System by WECC.

5. Effective Date: See Implementation Plan

6. Background: This standard uses three types of requirements to provide layers of protection to prevent vegetation related outages that could lead to Cascading:

a) Performance-based defines a particular reliability objective or outcome to be achieved. In its simplest form, a results-based requirement has four components: *who, under what conditions (if any), shall perform what action, to achieve what particular bulk power system performance result or outcome?*

b) Risk-based preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: *who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?*

c) Competency-based defines a minimum set of capabilities an entity needs to have to demonstrate it is able to perform its designated reliability functions. A competency-based reliability requirement should be framed as: *who, under what*

[2] *Id.*

[3] "Clear line of sight" means the distance that can be seen by the average person without special instrumentation (e.g., binoculars, telescope, spyglasses, etc.) on a clear day.

conditions (if any), shall have what capability, to achieve what particular result or outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the bulk power system?

The defense-in-depth strategy for Rreliability Sstandards development recognizes that each requirement in a NERC Rreliability Sstandard has a role in preventing system failures, and that these roles are complementary and reinforcing. Reliability Sstandards should not be viewed as a body of unrelated requirements, but rather should be viewed as part of a portfolio of requirements designed to achieve an overall defense-in-depth strategy and comport with the quality objectives of a Rreliability Sstandard.

This standard uses a defense-in-depth approach to improve the reliability of the electric Transmission system by:

- Requiring that vegetation be managed to prevent vegetation encroachment inside the flash-over clearance (R1 and R2);
- Requiring documentation of the maintenance strategies, procedures, processes and specifications used to manage vegetation to prevent potential flash-over conditions including consideration of 1) conductor dynamics and 2) the interrelationships between vegetation growth rates, control methods and the inspection frequency (R3);
- Requiring timely notification to the appropriate control center of vegetation conditions that could cause a flash-over at any moment (R4);
- Requiring corrective actions to ensure that flash-over distances will not be violated due to work constrains such as legal injunctions (R5);
- Requiring inspections of vegetation conditions to be performed annually (R6); and
- Requiring that the annual work needed to prevent flash-over is completed (R7).

For this standard, the requirements have been developed as follows:

- Performance-based: Requirements 1 and 2
- Competency-based: Requirement 3
- Risk-based: Requirements 4, 5, 6 and 7

Requirement R3 serves as the first line of defense by ensuring that entities understand the problem they are trying to manage and have fully developed strategies and plans to manage the problem. Requirements R1, R2, and R7 serve as the second line of defense by requiring that entities carry out their plans and manage vegetation. Requirement R6, which requires inspections, may be either a part of the first line of defense (as input into the strategies and plans) or as a third line of defense (as a check of the first and second lines of defense). Requirement R4 serves as the final line of defense, as it addresses cases in which all the other lines of defense have failed.

Major outages and operational problems have resulted from interference between overgrown vegetation and transmission lines located on many types of lands and ownership situations. Adherence to the standard requirements for applicable lines on any kind of land or easement, whether they are Federal Lands, state or provincial lands, public or private lands, franchises, easements or lands owned in fee, will reduce and manage this risk. For the purpose of the standard the term "public lands" includes municipal lands, village lands, city lands, and a host of other governmental entities.

This standard addresses vegetation management along applicable overhead lines and does not apply to underground lines, submarine lines or to line sections inside an electric station boundary.

This standard focuses on transmission lines to prevent those vegetation related outages that could lead to Cascading. It is not intended to prevent customer outages due to tree contact with lower voltage distribution system lines. For example, localized customer service might be disrupted if vegetation were to make contact with a 69kV transmission line supplying power to a 12kV distribution station. However, this standard is not written to address such isolated situations which have little impact on the overall electric transmission system.

Since vegetation growth is constant and always present, unmanaged vegetation poses an increased outage risk, especially when numerous transmission lines are operating at or near their Rating. This can present a significant risk of consecutive line failures when lines are experiencing large sags thereby leading to Cascading. Once the first line fails the shift of the current to the other lines and/or the increasing system loads will lead to the second and subsequent line failures as contact to the vegetation under those lines occurs. Conversely, most other outage causes (such as trees falling into lines, lightning, animals, motor vehicles, etc.) are not an interrelated function of the shift of currents or the increasing system loading. These events are not any more likely to occur during heavy system loads than any other time. There is no cause-effect relationship which creates the probability of simultaneous occurrence of other such events. Therefore these types of events are highly unlikely to cause large-scale grid failures. Thus, this standard places the highest priority on the management of vegetation to prevent vegetation grow-ins.

B. Requirements and Measures

R1. Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the Minimum Vegetation Clearance Distance (MVCD) of its applicable line(s), ~~which are either an element of an IROL, or an element of a Major WECC Transfer Path;~~ operating within their Rating and all

Rated Electrical Operating Conditions of the types shown below[4] *[Violation Risk Factor: High] [Time Horizon: Real-time]*:

1.1. An encroachment into the MVCD as shown in FAC-003-Table 2, observed in Real-time, absent a Sustained Outage,[5]

1.2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,[6]

1.3. An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage[7],

1.4. An encroachment due to vegetation growth into the MVCD that caused a vegetation-related Sustained Outage.[8]

M1. Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R1. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments. (R1)

R2. [Reserved for future use] ~~Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the MVCD of its applicable line(s) which are not either an element of an IROL, or an element of a Major WECC Transfer Path; operating within its Rating and all Rated Electrical Operating Conditions of the types shown below[9] *[Violation Risk Factor: High] [Time Horizon: Real-time]:*~~

~~**2.1.** An encroachment into the MVCD, observed in Real-time, absent a Sustained Outage,[10]~~

[4] This requirement does not apply to circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner subject to this R~~r~~eliability S~~s~~tandard, including natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, wind shear, fresh gale, major storms as defined either by the applicable Transmission Owner or applicable Generator Owner or an applicable regulatory body, ice storms, and floods; human or animal activity such as logging, animal severing tree, vehicle contact with tree, or installation, removal, or digging of vegetation. Nothing in this footnote should be construed to limit the Transmission Owner's or applicable Generator Owner's right to exercise its full legal rights on the ROW.

[5] If a later confirmation of a Fault by the applicable Transmission Owner or applicable Generator Owner shows that a vegetation encroachment within the MVCD has occurred from vegetation within the ROW, this shall be considered the equivalent of a Real-time observation.

[6] Multiple Sustained Outages on an individual line, if caused by the same vegetation, will be reported as one outage regardless of the actual number of outages within a 24-hour period.

[7] *Id.*

[8] *Id.*

~~[9] See footnote 4.~~

~~[10] See footnote 5.~~

~~2.2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,[11]~~

~~2.3. An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage,[12]~~

~~2.4.~~2.1. ~~An encroachment due to vegetation growth into the line MVCD that caused a vegetation-related Sustained Outage.[13]~~

M2. [Reserved for future use] ~~Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R2. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments. (R2)~~

R3. Each applicable Transmission Owner and applicable Generator Owner shall have documented maintenance strategies or procedures or processes or specifications it uses to prevent the encroachment of vegetation into the MVCD of its applicable lines that accounts for the following: *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]:*

3.1. Movement of applicable line conductors under their Rating and all Rated Electrical Operating Conditions;

3.2. Inter-relationships between vegetation growth rates, vegetation control methods, and inspection frequency.

M3. The maintenance strategies or procedures or processes or specifications provided demonstrate that the applicable Transmission Owner and applicable Generator Owner can prevent encroachment into the MVCD considering the factors identified in the requirement. (R3)

R4. Each applicable Transmission Owner and applicable Generator Owner, without any intentional time delay, shall notify the control center holding switching authority for the associated applicable line when the applicable Transmission Owner and applicable Generator Owner has confirmed the existence of a vegetation condition that is likely to cause a Fault at any moment *[Violation Risk Factor: Medium] [Time Horizon: Real-time].*

M4. Each applicable Transmission Owner and applicable Generator Owner that has a confirmed vegetation condition likely to cause a Fault at any moment will have evidence that it notified the control center holding switching authority for the

~~[11] See footnote 6.~~
~~[12] *Id.*~~

~~[13] *Id.*~~

associated transmission line without any intentional time delay. Examples of evidence may include control center logs, voice recordings, switching orders, clearance orders and subsequent work orders. (R4)

R5. When an applicable Transmission Owner and an applicable Generator Owner are constrained from performing vegetation work on an applicable line operating within its Rating and all Rated Electrical Operating Conditions, and the constraint may lead to a vegetation encroachment into the MVCD prior to the implementation of the next annual work plan, then the applicable Transmission Owner or applicable Generator Owner shall take corrective action to ensure continued vegetation management to prevent encroachments [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].

M5. Each applicable Transmission Owner and applicable Generator Owner has evidence of the corrective action taken for each constraint where an applicable transmission line was put at potential risk. Examples of acceptable forms of evidence may include initially-planned work orders, documentation of constraints from landowners, court orders, inspection records of increased monitoring, documentation of the de-rating of lines, revised work orders, invoices, or evidence that the line was de-energized. (R5)

R6. Each applicable Transmission Owner and applicable Generator Owner shall perform a Vegetation Inspection of 100% of its applicable transmission lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.) at least once per calendar year and with no more than 18 calendar months between inspections on the same ROW[14] [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].

M6. Each applicable Transmission Owner and applicable Generator Owner has evidence that it conducted Vegetation Inspections of the transmission line ROW for all applicable lines at least once per calendar year but with no more than 18 calendar months between inspections on the same ROW. Examples of acceptable forms of evidence may include completed and dated work orders, dated invoices, or dated inspection records. (R6)

R7. Each applicable Transmission Owner and applicable Generator Owner shall complete 100% of its annual vegetation work plan of applicable lines to ensure no vegetation encroachments occur within the MVCD. Modifications to the work plan in response to changing conditions or to findings from vegetation inspections may be made (provided they do not allow encroachment of vegetation into the MVCD) and must be documented. The percent completed calculation is based on the number of units actually completed divided by the number of units in the final amended plan (measured in units of choice - circuit, pole line, line miles or kilometers, etc.).

[14] When the applicable Transmission Owner or applicable Generator Owner is prevented from performing a Vegetation Inspection within the timeframe in R6 due to a natural disaster, the TO or GO is granted a time extension that is equivalent to the duration of the time the TO or GO was prevented from performing the Vegetation Inspection.

Examples of reasons for modification to annual plan may include [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*]:

7.1. Change in expected growth rate/environmental factors

7.2. Circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner[15]

7.3. Rescheduling work between growing seasons

7.4. Crew or contractor availability/Mutual assistance agreements

7.5. Identified unanticipated high priority work

7.6. Weather conditions/Accessibility

7.7. Permitting delays

7.8. Land ownership changes/Change in land use by the landowner

7.9. Emerging technologies

M7. Each applicable Transmission Owner and applicable Generator Owner has evidence that it completed its annual vegetation work plan for its applicable lines. Examples of acceptable forms of evidence may include a copy of the completed annual work plan (as finally modified), dated work orders, dated invoices, or dated inspection records. (R7)

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.

[15] Circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner include but are not limited to natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, ice storms, floods, or major storms as defined either by the TO or GO or an applicable regulatory body.

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 applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirements R1, R2, R3, R5, R6 and R7, for three calendar years.
- The applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirement R4, Measure M4 for most recent 12 months of operator logs or most recent 3 months of voice recordings or transcripts of voice recordings, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- If an applicable Transmission Owner or applicable Generator Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time period specified above, whichever is longer.

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

Periodic Data Submittal: The applicable Transmission Owner and applicable Generator Owner will submit a quarterly report to its Regional Entity, or the Regional Entity's designee, identifying all Sustained Outages of applicable lines operated within their Rating and all Rated Electrical Operating Conditions as determined by the applicable Transmission Owner or applicable Generator Owner to have been caused by vegetation, except as excluded in footnote 2, and including as a minimum the following:

- The name of the circuit(s), the date, time and duration of the outage; the voltage of the circuit; a description of the cause of the outage; the category associated with the Sustained Outage; other pertinent comments; and any countermeasures taken by the applicable Transmission Owner or applicable Generator Owner.

  A Sustained Outage is to be categorized as one of the following:

- Category 1A — Grow-ins: Sustained Outages caused by vegetation growing into applicable lines, that are identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only), as Facilities that if lost or degraded are expected to result in instances of instability,

Cascading, or uncontrolled separation~~as an element of an IROL or Major WECC Transfer Path~~, by vegetation inside and/or outside of the ROW;

- Category 1B — Grow-ins: Sustained Outages caused by vegetation growing into applicable lines, but are not identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lostor degraded are expected to result in instances of instability, Cascading, or uncontrolled separation~~as an element of an IROL or Major WECC Transfer Path~~, by vegetation inside and/or outside of the ROW;
- Category 2A — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines that are identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are epected to result in instances of instability, Cascading, or uncontrolled separation~~as an element of an IROL or Major WECC Transfer Path~~, from within the ROW;
- Category 2B — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines, but are not identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation~~as an element of an IROL or Major WECC Transfer Path~~, from within the ROW;
- Category 3 — Fall-ins: Sustained Outages caused by vegetation falling into applicable lines from outside the ROW;
- Category 4A — Blowing together: Sustained Outages caused by vegetation and applicable lines that are identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation~~as an element of an IROL or Major WECC Transfer Path~~, blowing together from within the ROW;
- Category 4B — Blowing together: Sustained Outages caused by vegetation and applicable lines, but are not identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation~~as an element of an IROL or Major WECC Transfer Path~~, blowing together from within the ROW.

The Regional Entity will report the outage information provided by applicable Transmission Owners and applicable Generator Owners, as per

the above, quarterly to NERC, as well as any actions taken by the Regional Entity as a result of any of the reported Sustained Outages.

Violation Severity Levels (Table 1)

R #	Table 1: Violation Severity Levels (VSL)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation ~~as an element of an IROL or Major WECC transfer path~~ and encroachment into the MVCD as identified in FAC-003-4-Table 2 was observed in real time absent a Sustained Outage.	The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line identified by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation ~~as an element of an IROL or Major WECC transfer path~~ and a vegetation-related Sustained Outage was caused by one of the following: • *A fall-in from inside the active transmission line ROW*

				• *Blowing together of applicable lines and vegetation located inside the active transmission line ROW* • *A grow-in*
R2.			~~The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line not identified as an element of an IROL or Major WECC transfer path and encroachment into the MVCD as identified in FAC-003-4 Table 2 was observed in real time absent a Sustained Outage.~~	~~The responsible entity failed to manage vegetation to prevent encroachment into the MVCD of a line not identified as an element of an IROL or Major WECC transfer path and a vegetation-related Sustained Outage was caused by one of the following:~~ • ~~*A fall-in from inside the active transmission line ROW*~~ • ~~*Blowing together of applicable lines and vegetation located inside the active transmission line ROW*~~ • ~~*A grow-in*~~
R3.		The responsible entity has maintenance strategies or documented procedures or	The responsible entity has maintenance strategies or documented procedures or	The responsible entity does not have any maintenance strategies or documented

		processes or specifications but has not accounted for the inter-relationships between vegetation growth rates, vegetation control methods, and inspection frequency, for the responsible entity's applicable lines. (Requirement R3, Part 3.2.)	processes or specifications but has not accounted for the movement of transmission line conductors under their Rating and all Rated Electrical Operating Conditions, for the responsible entity's applicable lines. (Requirement R3, Part 3.1.)	procedures or processes or specifications used to prevent the encroachment of vegetation into the MVCD, for the responsible entity's applicable lines.
R4.			The responsible entity experienced a confirmed vegetation threat and notified the control center holding switching authority for that applicable line, but there was intentional delay in that notification.	The responsible entity experienced a confirmed vegetation threat and did not notify the control center holding switching authority for that applicable line.
R5.				The responsible entity did not take corrective action when it was constrained from performing planned vegetation work where an applicable line was put at potential risk.
R6.	The responsible entity failed to inspect 5% or less of its applicable lines (measured in units of choice - circuit, pole	The responsible entity failed to inspect more than 5% up to and including 10% of its applicable lines (measured in	The responsible entity failed to inspect more than 10% up to and including 15% of its applicable lines (measured in	The responsible entity failed to inspect more than 15% of its applicable lines (measured in units of choice

	line, line miles or kilometers, etc.)	units of choice - circuit, pole line, line miles or kilometers, etc.).	units of choice - circuit, pole line, line miles or kilometers, etc.).	- circuit, pole line, line miles or kilometers, etc.).
R7.	The responsible entity failed to complete 5% or less of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 5% and up to and including 10% of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 10% and up to and including 15% of its annual vegetation work plan for its applicable lines (as finally modified).	The responsible entity failed to complete more than 15% of its annual vegetation work plan for its applicable lines (as finally modified).

D. Regional Variances

None.

E. Associated Documents

- FAC-003-4 Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	January 20, 2006	1. Added “Standard Development Roadmap.” 2. Changed “60” to “Sixty” in section A, 5.2. 3. Added “Proposed Effective Date: April 7, 2006” to footer. 4. Added “Draft 3: November 17, 2005” to footer.	New
1	April 4, 2007	Regulatory Approval - Effective Date	New

2	November 3, 2011	Adopted by the NERC Board of Trustees	New
2	March 21, 2013	FERC Order issued approving FAC-003-2 (Order No. 777) FERC Order No. 777 was issued on March 21, 2013 directing NERC to "conduct or contract testing to obtain empirical data and submit a report to the Commission providing the results of the testing."[16]	Revisions
2	May 9, 2013	Board of Trustees adopted the modification of the VRF for Requirement R2 of FAC-003-2 by raising the VRF from "Medium" to "High."	Revisions
3	May 9, 2013	FAC-003-3 adopted by Board of Trustees	Revisions
3	September 19, 2013	A FERC order was issued on September 19, 2013, approving FAC-003-3. This standard became enforceable on July 1, 2014 for Transmission Owners. For Generator Owners, R3 became enforceable on January 1, 2015 and all other requirements (R1, R2, R4, R5, R6, and R7) became enforceable on January 1, 2016.	Revisions
3	November 22, 2013	Updated the VRF for R2 from "Medium" to "High" per a Final Rule issued by FERC	Revisions
3	July 30, 2014	Transferred the effective dates section from FAC-003-2 (for Transmission Owners) into FAC-003-3, per the FAC-003-3 implementation plan	Revisions

[16] *Revisions to Reliability Standard for Transmission Vegetation Management, Order No. 777,* 142 FERC ¶ 61,208 (2013)

4	February 11, 2016	Adopted by Board of Trustees. Adjusted MVCD values in Table 2 for alternating current systems, consistent with findings reported in report filed on August 12, 2015 in Docket No. RM12-4-002 consistent with FERC's directive in Order No. 777, and based on empirical testing results for flashover distances between conductors and vegetation.	Revisions
4	March 9, 2016	Corrected subpart 7.10 to M7, corrected value of .07 to .7	Errata
4	April 26, 2016	FERC Letter Order approving FAC-003-4. Docket No. RD16-4-000.	

FAC-003 — TABLE 2 — Minimum Vegetation Clearance Distances (MVCD)[17]

For **Alternating Current** Voltages (feet)

(AC) Nominal System Voltage (KV)+	(AC) Maximum System Voltage (kV)[18]	MVCD (feet) Over sea level up to 500 ft	MVCD feet Over 500 ft up to 1000 ft	MVCD feet Over 1000 ft up to 2000 ft	MVCD feet Over 2000 ft up to 3000 ft	MVCD feet Over 3000 ft up to 4000 ft	MVCD feet Over 4000 ft up to 5000 ft	MVCD feet Over 5000 ft up to 6000 ft	MVCD feet Over 6000 ft up to 7000 ft	MVCD feet Over 7000 ft up to 8000 ft	MVCD feet Over 8000 ft up to 9000 ft	MVCD feet Over 9000 ft up to 10000 ft	MVCD feet Over 10000 ft up to 11000 ft	MVCD feet Over 11000 ft up to 12000 ft	MVCD feet Over 12000 ft up to 13000 ft	MVCD feet Over 13000 ft up to 14000 ft	MVCD feet Over 14000 ft up to 15000 ft
765	800	11.6ft	11.7ft	11.9ft	12.1ft	12.2ft	12.4ft	12.6ft	12.8ft	13.0ft	13.1ft	13.3ft	13.5ft	13.7ft	13.9ft	14.1ft	14.3ft
500	550	7.0ft	7.1ft	7.2ft	7.4ft	7.5ft	7.6ft	7.8ft	7.9ft	8.1ft	8.2ft	8.3ft	8.5ft	8.6ft	8.8ft	8.9ft	9.1ft
345	362[19]	4.3ft	4.3ft	4.4ft	4.5ft	4.6ft	4.7ft	4.8ft	4.9ft	5.0ft	5.1ft	5.2ft	5.3ft	5.4ft	5.5ft	5.6ft	5.7ft
287	302	5.2ft	5.3ft	5.4ft	5.5ft	5.6ft	5.7ft	5.8ft	5.9ft	6.1ft	6.2ft	6.3ft	6.4ft	6.5ft	6.6ft	6.8ft	6.9ft
230	242	4.0ft	4.1ft	4.2ft	4.3ft	4.3ft	4.4ft	4.5ft	4.6ft	4.7ft	4.8ft	4.9ft	5.0ft	5.1ft	5.2ft	5.3ft	5.4ft
161*	169	2.7ft	2.7ft	2.8ft	2.9ft	2.9ft	3.0ft	3.0ft	3.1ft	3.2ft	3.3ft	3.3ft	3.4ft	3.5ft	3.6ft	3.7ft	3.8ft
138*	145	2.3ft	2.3ft	2.4ft	2.4ft	2.5ft	2.5ft	2.6ft	2.7ft	2.7ft	2.8ft	2.8ft	2.9ft	3.0ft	3.0ft	3.1ft	3.2ft
115*	121	1.9ft	1.9ft	1.9ft	2.0ft	2.0ft	2.1ft	2.1ft	2.2ft	2.2ft	2.3ft	2.3ft	2.4ft	2.5ft	2.5ft	2.6ft	2.7ft
88*	100	1.5ft	1.5ft	1.6ft	1.6ft	1.7ft	1.7ft	1.8ft	1.8ft	1.8ft	1.9ft	1.9ft	2.0ft	2.0ft	2.1ft	2.2ft	2.2ft
69*	72	1.1ft	1.1ft	1.1ft	1.2ft	1.2ft	1.2ft	1.2ft	1.3ft	1.3ft	1.3ft	1.4ft	1.4ft	1.4ft	1.5ft	1.6ft	1.6ft

* Such lines are applicable to this standard only if PC has determined such per FAC-014 (refer to the Applicability Section above)

[17] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

[18] Where applicable lines are operated at nominal voltages other than those listed, the applicable Transmission Owner or applicable Generator Owner should use the maximum system voltage to determine the appropriate clearance for that line.

[19] The change in transient overvoltage factors in the calculations are the driver in the decrease in MVCDs for voltages of 345 kV and above. Refer to pp.29-31 in the Supplemental Materials for additional information.

[+] *Table 2 – Table of MVCD values at a 1.0 gap factor (in U.S. customary units), which is located in the EPRI report filed with FERC on August 12, 2015. (The 14000-15000 foot values were subsequently provided by EPRI in an updated Table 2 on December 1, 2015, filed with the FAC-003-4 Petition at FERC)*

TABLE 2 (CONT) — Minimum Vegetation Clearance Distances (MVCD)[20]

For **Alternating Current** Voltages (meters)

(AC) Nominal System Voltage (KV)[+]	(AC) Maximum System Voltage (kV)[21]	MVCD meters Over sea level up to 153 m	MVCD meters Over 153m up to 305m	MVCD meters Over 305m up to 610m	MVCD meters Over 610m up to 915m	MVCD meters Over 915m up to 1220m	MVCD meters Over 1220m up to 1524m	MVCD meters Over 1524m up to 1829m	MVCD meters Over 1829m up to 2134m	MVCD meters Over 2134m up to 2439m	MVCD meters Over 2439m up to 2744m	MVCD meters Over 2744m up to 3048m	MVCD meters Over 3048m up to 3353m	MVCD meters Over 3353m up to 3657m	MVCD meters Over 3657m up to 3962m	MVCD meters Over 3962 m up to 4268 m	MVCD meters Over 4268 m up to 4572 m
765	800	3.6m	3.6m	3.6m	3.7m	3.7m	3.8m	3.8m	3.9m	4.0m	4.0m	4.1m	4.1m	4.2m	4.2m	4.3m	4.4m
500	550	2.1m	2.2m	2.2m	2.3m	2.3m	2.3m	2.4m	2.4m	2.5m	2..5m	2.5m	2.6m	2.6m	2.7m	2.7m	2.7m
345	362[22]	1.3m	1.3m	1.3m	1.4m	1.4m	1.4m	1.5m	1.5m	1.5m	1.6m	1.6m	1.6m	1.6m	1.7m	1.7m	1.8m
287	302	1.6m	1.6m	1.7m	1.7m	1.7m	1.7m	1.8m	1.8m	1.9m	1.9m	1.9m	2.0m	2.0m	2.0m	2.1m	2.1m
230	242	1.2m	1.3m	1.3m	1.3m	1.3m	1.3m	1.4m	1.4m	1.4m	1.5m	1.5m	1.5m	1.6m	1.6m	1.6m	1.6m
161*	169	0.8m	0.8m	0.9m	0.9m	0.9m	0.9m	0.9m	1.0m	1.0m	1.0m	1.0m	1.0m	1.1m	1.1m	1.1m	1.1m
138*	145	0.7m	0.7m	0.7m	0.7m	0.7m	0.7m	0.8m	0.8m	0.8m	0.9m	0.9m	0.9m	0.9m	0.9m	1.0m	1.0m
115*	121	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.7m	0.7m	0.7m	0.7m	0.7m	0.8m	0.8m	0.8m	0.8m
88*	100	0.4m	0.4m	0.5m	0.5m	0.5m	0.5m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.6m	0.7m	0.7m
69*	72	0.3m	0.3m	0.3m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.4m	0.5m	0.5m	0.5m

* Such lines are applicable to this standard only if PC has determined such per FAC-014 (refer to the Applicability Section above)

[20] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

[21] Where applicable lines are operated at nominal voltages other than those listed, the applicable Transmission Owner or applicable Generator Owner should use the maximum system voltage to determine the appropriate clearance for that line.

[22] The change in transient overvoltage factors in the calculations are the driver in the decrease in MVCDs for voltages of 345 kV and above. Refer to pp.29-31 in the supplemental materials for additional information.

[+] Table 2 – Table of MVCD values at a 1.0 gap factor (in U.S. customary units), which is located in the EPRI report filed with FERC on August 12, 2015. (The 14000-15000 foot values were subsequently provided by EPRI in an updated Table 2 on December 1, 2015, filed with the FAC-003-4 Petition at FERC)

TABLE 2 (CONT) — Minimum Vegetation Clearance Distances (MVCD)[23]

For **Direct Current** Voltages feet (meters)

(DC) Nominal Pole to Ground Voltage (kV)	MVCD meters Over sea level up to 500 ft (Over sea level up to 152.4 m)	MVCD meters Over 500 ft up to 1000 ft (Over 152.4 m up to 304.8 m	MVCD meters Over 1000 ft up to 2000 ft (Over 304.8 m up to 609.6m)	MVCD meters Over 2000 ft up to 3000 ft (Over 609.6m up to 914.4m	MVCD meters Over 3000 ft up to 4000 ft (Over 914.4m up to 1219.2m	MVCD meters Over 4000 ft up to 5000 ft (Over 1219.2m up to 1524m	MVCD meters Over 5000 ft up to 6000 ft (Over 1524 m up to 1828.8 m)	MVCD meters Over 6000 ft up to 7000 ft (Over 1828.8m up to 2133.6m)	MVCD meters Over 7000 ft up to 8000 ft (Over 2133.6m up to 2438.4m)	MVCD meters Over 8000 ft up to 9000 ft (Over 2438.4m up to 2743.2m)	MVCD meters Over 9000 ft up to 10000 ft (Over 2743.2m up to 3048m)	MVCD meters Over 10000 ft up to 11000 ft (Over 3048m up to 3352.8m)
±750	14.12ft (4.30m)	14.31ft (4.36m)	14.70ft (4.48m)	15.07ft (4.59m)	15.45ft (4.71m)	15.82ft (4.82m)	16.2ft (4.94m)	16.55ft (5.04m)	16.91ft (5.15m)	17.27ft (5.26m)	17.62ft (5.37m)	17.97ft (5.48m)
±600	10.23ft (3.12m)	10.39ft (3.17m)	10.74ft (3.26m)	11.04ft (3.36m)	11.35ft (3.46m)	11.66ft (3.55m)	11.98ft (3.65m)	12.3ft (3.75m)	12.62ft (3.85m)	12.92ft (3.94m)	13.24ft (4.04m)	13.54ft (4.13m)
±500	8.03ft (2.45m)	8.16ft (2.49m)	8.44ft (2.57m)	8.71ft (2.65m)	8.99ft (2.74m)	9.25ft (2.82m)	9.55ft (2.91m)	9.82ft (2.99m)	10.1ft (3.08m)	10.38ft (3.16m)	10.65ft (3.25m)	10.92ft (3.33m)
±400	6.07ft (1.85m)	6.18ft (1.88m)	6.41ft (1.95m)	6.63ft (2.02m)	6.86ft (2.09m)	7.09ft (2.16m)	7.33ft (2.23m)	7.56ft (2.30m)	7.80ft (2.38m)	8.03ft (2.45m)	8.27ft (2.52m)	8.51ft (2.59m)
±250	3.50ft (1.07m)	3.57ft (1.09m)	3.72ft (1.13m)	3.87ft (1.18m)	4.02ft (1.23m)	4.18ft (1.27m)	4.34ft (1.32m)	4.5ft (1.37m)	4.66ft (1.42m)	4.83ft (1.47m)	5.00ft (1.52m)	5.17ft (1.58m)

[23] The distances in this Table are the minimums required to prevent Flash-over; however prudent vegetation maintenance practices dictate that substantially greater distances will be achieved at time of vegetation maintenance.

Guideline and Technical Basis

Effective dates:

The Compliance section is standard language used in most NERC standards to cover the general effective date and covers the vast majority of situations. A special case covers effective dates for (1) lines initially becoming subject to the Standard, (2) lines changing in applicability within the standard.

The special case is needed because the Planning Coordinators may designate lines below 200 kV-, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation, ~~to become elements of an IROL or Major WECC Transfer Path~~ in a future Planning Year (PY). For example, studies by the Planning Coordinator in 2015 may identify a line to have that designation beginning in PY 2025, ten years after the planning study is performed. It is not intended for the Standard to be immediately applicable to, or in effect for, that line until that future PY begins. The effective date provision for such lines ensures that the line will become subject to the standard on January 1 of the PY specified with an allowance of at least 12 months for the applicable Transmission Owner or applicable Generator Owner to make the necessary preparations to achieve compliance on that line. A line operating below 200kV designated by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation ~~as an element of an IROL or Major WECC Transfer Path~~ may be removed from that designation due to system improvements, changes in generation, changes in loads or changes in studies and analysis of the network.

Date that Planning Study is completed	PY the line will become an ~~IROL~~ identified element	Date 1	Date 2	Effective Date The later of Date 1 or Date 2
05/15/2011	2012	05/15/2012	01/01/2012	05/15/2012
05/15/2011	2013	05/15/2012	01/01/2013	01/01/2013
05/15/2011	2014	05/15/2012	01/01/2014	01/01/2014
05/15/2011	2021	05/15/2012	01/01/2021	01/01/2021

Defined Terms:

Explanation for revising the definition of ROW:

The current NERC glossary definition of Right of Way has been modified to include Generator Owners and to address the matter set forth in Paragraph 734 of FERC Order 693. The Order pointed out that Transmission Owners may in some cases own more property or rights than are needed to reliably operate transmission lines. This definition represents a slight but significant departure from the strict legal definition of "right of way" in that this definition is based on engineering and construction considerations that establish the width of a corridor from a technical basis. The pre-2007 maintenance records are included in the current definition to allow the use of such vegetation widths if there were no engineering or construction standards that referenced the width of right of way to be maintained for vegetation on a particular line but the evidence exists in maintenance records for a width that was in fact maintained prior to this standard becoming mandatory. Such widths may be the only information available for lines that had limited or no vegetation easement rights and were typically maintained primarily to ensure public safety. This standard does not require additional easement rights to be purchased to satisfy a minimum right of way width that did not exist prior to this standard becoming mandatory.

Explanation for revising the definition of Vegetation Inspection:
The current glossary definition of this NERC term was modified to include Generator Owners and to allow both maintenance inspections and vegetation inspections to be performed concurrently. This allows potential efficiencies, especially for those lines with minimal vegetation and/or slow vegetation growth rates.

Explanation of the derivation of the MVCD:
The MVCD is a calculated minimum distance that is derived from the Gallet equation. This is a method of calculating a flash over distance that has been used in the design of high voltage transmission lines. Keeping vegetation away from high voltage conductors by this distance will prevent voltage flash-over to the vegetation. See the explanatory text below for Requirement R3 and associated Figure 1. Table 2 of the ~~S~~standard provides MVCD values for various voltages and altitudes. The table is based on empirical testing data from EPRI as requested by FERC in Order No. 777.

Project 2010-07.1 Adjusted MVCDs per EPRI Testing:
In Order No. 777, FERC directed NERC to undertake testing to gather empirical data validating the appropriate gap factor used in the Gallet equation to calculate MVCDs, specifically the gap factor for the flash-over distances between conductors and vegetation. See, Order No. 777, at P 60. NERC engaged industry through a collaborative research project and contracted EPRI to complete the scope of work. In January 2014, NERC formed an advisory group to assist with developing the scope of work for the project. This team provided subject matter expertise for developing the test plan, monitoring testing, and vetting the analysis and conclusions to be submitted in a final report. The advisory team was comprised of NERC staff, arborists, and industry members with wide-ranging expertise in transmission engineering, insulation coordination, and vegetation management. The testing project commenced in April 2014 and continued through October 2014 with the final set of testing completed in May 2015. Based on these testing results conducted by EPRI, and consistent with the report filed in FERC Docket No.

RM12-4-000, the gap factor used in the Gallet equation required adjustment from 1.3 to 1.0. This resulted in increased MVCD values for all alternating current system voltages identified. The adjusted MVCD values, reflecting the 1.0 gap factor, are included in Table 2 of version 4 of FAC-003.

The air gap testing completed by EPRI per FERC Order No. 777 established that trees with large spreading canopies growing directly below energized high voltage conductors create the greatest likelihood of an air gap flash over incident and was a key driver in changing the gap factor to a more conservative value of 1.0 in version 4 of this standard.

Requirements R1 and R2:

R1 and R2 are performance-based requirements. The reliability objective or outcome to be achieved is the management of vegetation such that there are no vegetation encroachments within a minimum distance of transmission lines. Content-wise, R1 and R2 are the same requirements; however, they apply to different Facilities. Both R1 and R2 require each applicable Transmission Owner or applicable Generator Owner to manage vegetation to prevent encroachment within the MVCD of transmission lines. R1 is applicable to lines that are identified as an element ~~of an IROL or Major WECC Transfer Path~~by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation. R2 is applicable to all other lines that are not identified as an element by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lost or degraded are expected to result in instances of instability, Cascading, or uncontrolled separation~~pursuant to FAC-015-1 Requirement R4elements of IROLs, and not elements of Major WECC Transfer Paths~~.

The separation of applicability (between R1 and R2) recognizes that inadequate vegetation management for an applicable line has been identified as an element by the Planning Coordinator, per its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability Assessment (Planning Coordinator only) as Facilities that if lostor degraded are expected to result in instances of instability, Cascading, or uncontrolled separation~~that is an element of an IROL or a Major WECC Transfer Path~~ is a greater risk to the interconnected electric transmission system than applicable lines that ~~are not elements of IROLs or Major WECC Transfer Paths~~have not been identified as such. Applicable lines that ~~are not elements of IROLs or Major WECC Transfer Paths~~have not been identified as such do require effective vegetation management, but these lines are comparatively less operationally significant.

Requirements R1 and R2 state that if inadequate vegetation management allows vegetation to encroach within the MVCD distance as shown in Table 2, it is a violation of the standard. Table 2 distances are the minimum clearances that will prevent spark-over based on the Gallet equations. These requirements assume that transmission lines and their conductors are operating within their Rating. If a line conductor is intentionally or inadvertently operated beyond its Rating and Rated Electrical Operating Condition (potentially in violation of other standards), the occurrence

of a clearance encroachment may occur solely due to that condition. For example, emergency actions taken by an applicable Transmission Owner or applicable Generator Owner or Reliability Coordinator to protect an Interconnection may cause excessive sagging and an outage. Another example would be ice loading beyond the line's Rating and Rated Electrical Operating Condition. Such vegetation-related encroachments and outages are not violations of this standard.

Evidence of failures to adequately manage vegetation include real-time observation of a vegetation encroachment into the MVCD (absent a Sustained Outage), or a vegetation-related encroachment resulting in a Sustained Outage due to a fall-in from inside the ROW, or a vegetation-related encroachment resulting in a Sustained Outage due to the blowing together of the lines and vegetation located inside the ROW, or a vegetation-related encroachment resulting in a Sustained Outage due to a grow-in. Faults which do not cause a Sustained outage and which are confirmed to have been caused by vegetation encroachment within the MVCD are considered the equivalent of a Real-time observation for violation severity levels.

With this approach, the VSLs for R1 and R2 are structured such that they directly correlate to the severity of a failure of an applicable Transmission Owner or applicable Generator Owner to manage vegetation and to the corresponding performance level of the Transmission Owner's vegetation program's ability to meet the objective of "preventing the risk of those vegetation related outages that could lead to Cascading." Thus violation severity increases with an applicable Transmission Owner's or applicable Generator Owner's inability to meet this goal and its potential of leading to a Cascading event. The additional benefits of such a combination are that it simplifies the standard and clearly defines performance for compliance. A performance-based requirement of this nature will promote high quality, cost effective vegetation management programs that will deliver the overall end result of improved reliability to the system.

Multiple Sustained Outages on an individual line can be caused by the same vegetation. For example initial investigations and corrective actions may not identify and remove the actual outage cause then another outage occurs after the line is re-energized and previous high conductor temperatures return. Such events are considered to be a single vegetation-related Sustained Outage under the standard where the Sustained Outages occur within a 24 hour period.

If the applicable Transmission Owner or applicable Generator Owner has applicable lines operated at nominal voltage levels not listed in Table 2, then the applicable TO or applicable GO should use the next largest clearance distance based on the next highest nominal voltage in the table to determine an acceptable distance.

Requirement R3:
R3 is a competency based requirement concerned with the maintenance strategies, procedures, processes, or specifications, an applicable Transmission Owner or applicable Generator Owner uses for vegetation management.

An adequate transmission vegetation management program formally establishes the approach the applicable Transmission Owner or applicable Generator Owner uses to plan and perform vegetation work to prevent transmission Sustained Outages and minimize risk to the transmission system. The approach provides the basis for evaluating the intent, allocation of appropriate resources, and the competency of the applicable Transmission Owner or applicable Generator Owner in managing vegetation. There are many acceptable approaches to manage vegetation and avoid Sustained Outages. However, the applicable Transmission Owner or applicable Generator Owner must be able to show the documentation of its approach and how it conducts work to maintain clearances.

An example of one approach commonly used by industry is ANSI Standard A300, part 7. However, regardless of the approach a utility uses to manage vegetation, any approach an applicable Transmission Owner or applicable Generator Owner chooses to use will generally contain the following elements:

1. *the maintenance strategy used (such as minimum vegetation-to-conductor distance or maximum vegetation height) to ensure that MVCD clearances are never violated*
2. *the work methods that the applicable Transmission Owner or applicable Generator Owner uses to control vegetation*
3. *a stated Vegetation Inspection frequency*
4. *an annual work plan*

The conductor's position in space at any point in time is continuously changing in reaction to a number of different loading variables. Changes in vertical and horizontal conductor positioning are the result of thermal and physical loads applied to the line. Thermal loading is a function of line current and the combination of numerous variables influencing ambient heat dissipation including wind velocity/direction, ambient air temperature and precipitation. Physical loading applied to the conductor affects sag and sway by combining physical factors such as ice and wind loading. The movement of the transmission line conductor and the MVCD is illustrated in Figure 1 below.

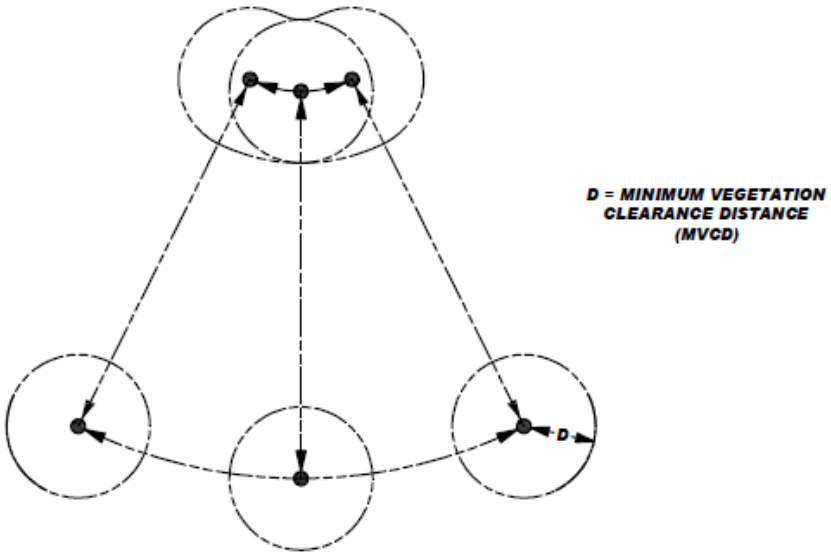


Figure 1

A cross-section view of a single conductor at a given point along the span is shown with six possible conductor positions due to movement resulting from thermal and mechanical loading.

Requirement R4:
R4 is a risk-based requirement. It focuses on preventative actions to be taken by the applicable Transmission Owner or applicable Generator Owner for the mitigation of Fault risk when a vegetation threat is confirmed. R4 involves the notification of potentially threatening vegetation conditions, without any intentional delay, to the control center holding switching authority for that specific transmission line. Examples of acceptable unintentional delays may include communication system problems (for example, cellular service or two-way radio disabled), crews located in remote field locations with no communication access, delays due to severe weather, etc.

Confirmation is key that a threat actually exists due to vegetation. This confirmation could be in the form of an applicable Transmission Owner or applicable Generator Owner employee who personally identifies such a threat in the field. Confirmation could also be made by sending out an employee to evaluate a situation reported by a landowner.

Vegetation-related conditions that warrant a response include vegetation that is near or encroaching into the MVCD (a grow-in issue) or vegetation that could fall into the transmission conductor (a fall-in issue). A knowledgeable verification of the risk would include an assessment of the possible sag or movement of the conductor while operating between no-load conditions and its rating.

The applicable Transmission Owner or applicable Generator Owner has the responsibility to ensure the proper communication between field personnel and the control center to allow the control center to take the appropriate action until or as the vegetation threat is relieved. Appropriate actions may include a temporary reduction in the line loading, switching the line out of service, or other preparatory actions in recognition of the increased risk of outage on that circuit. The notification of the threat should be communicated in terms of minutes or hours as opposed to a longer time frame for corrective action plans (see R5).

All potential grow-in or fall-in vegetation-related conditions will not necessarily cause a Fault at any moment. For example, some applicable Transmission Owners or applicable Generator Owners may have a danger tree identification program that identifies trees for removal with the potential to fall near the line. These trees would not require notification to the control center unless they pose an immediate fall-in threat.

Requirement R5:
R5 is a risk-based requirement. It focuses upon preventative actions to be taken by the applicable Transmission Owner or applicable Generator Owner for the mitigation of Sustained Outage risk when temporarily constrained from performing vegetation maintenance. The intent of this requirement is to deal with situations that prevent the applicable Transmission Owner or applicable Generator Owner from performing planned vegetation management work and, as a result, have the potential to put the transmission line at risk. Constraints to performing vegetation maintenance work as planned could result from legal injunctions filed by property owners, the discovery of easement stipulations which limit the applicable Transmission Owner's or applicable Generator Owner's rights, or other circumstances.

This requirement is not intended to address situations where the transmission line is not at potential risk and the work event can be rescheduled or re-planned using an alternate work methodology. For example, a land owner may prevent the planned use of herbicides to control incompatible vegetation outside of the MVCD, but agree to the use of mechanical clearing. In this case the applicable Transmission Owner or applicable Generator Owner is not under any immediate time constraint for achieving the management objective, can easily reschedule work using an alternate approach, and therefore does not need to take interim corrective action.

However, in situations where transmission line reliability is potentially at risk due to a constraint, the applicable Transmission Owner or applicable Generator Owner is required to take an interim corrective action to mitigate the potential risk to the transmission line. A wide range of actions can be taken to address various situations. General considerations include:

- Identifying locations where the applicable Transmission Owner or applicable Generator Owner is constrained from performing planned vegetation maintenance work which potentially leaves the transmission line at risk.
- Developing the specific action to mitigate any potential risk associated with not performing the vegetation maintenance work as planned.

- Documenting and tracking the specific action taken for the location.
- In developing the specific action to mitigate the potential risk to the transmission line the applicable Transmission Owner or applicable Generator Owner could consider location specific measures such as modifying the inspection and/or maintenance intervals. Where a legal constraint would not allow any vegetation work, the interim corrective action could include limiting the loading on the transmission line.
- The applicable Transmission Owner or applicable Generator Owner should document and track the specific corrective action taken at each location. This location may be indicated as one span, one tree or a combination of spans on one property where the constraint is considered to be temporary.

Requirement R6:
R6 is a risk-based requirement. This requirement sets a minimum time period for completing Vegetation Inspections. The provision that Vegetation Inspections can be performed in conjunction with general line inspections facilitates a Transmission Owner's ability to meet this requirement. However, the applicable Transmission Owner or applicable Generator Owner may determine that more frequent vegetation specific inspections are needed to maintain reliability levels, based on factors such as anticipated growth rates of the local vegetation, length of the local growing season, limited ROW width, and local rainfall. Therefore it is expected that some transmission lines may be designated with a higher frequency of inspections.

The VSLs for Requirement R6 have levels ranked by the failure to inspect a percentage of the applicable lines to be inspected. To calculate the appropriate VSL the applicable Transmission Owner or applicable Generator Owner may choose units such as: circuit, pole line, line miles or kilometers, etc.

For example, when an applicable Transmission Owner or applicable Generator Owner operates 2,000 miles of applicable transmission lines this applicable Transmission Owner or applicable Generator Owner will be responsible for inspecting all the 2,000 miles of lines at least once during the calendar year. If one of the included lines was 100 miles long, and if it was not inspected during the year, then the amount failed to inspect would be 100/2000 = 0.05 or 5%. The "Low VSL" for R6 would apply in this example.

Requirement R7:
R7 is a risk-based requirement. The applicable Transmission Owner or applicable Generator Owner is required to complete its annual work plan for vegetation management to accomplish the purpose of this standard. Modifications to the work plan in response to changing conditions or to findings from vegetation inspections may be made and documented provided they do not put the transmission system at risk. The annual work plan requirement is not intended to necessarily require a "span-by-span", or even a "line-by-line" detailed description of all work to be performed. It is only intended to require that the applicable Transmission Owner or applicable Generator Owner provide evidence of annual planning and execution of a vegetation

management maintenance approach which successfully prevents encroachment of vegetation into the MVCD.

When an applicable Transmission Owner or applicable Generator Owner identifies 1,000 miles of applicable transmission lines to be completed in the applicable Transmission Owner's or applicable Generator Owner's annual plan, the applicable Transmission Owner or applicable Generator Owner will be responsible completing those identified miles. If an applicable Transmission Owner or applicable Generator Owner makes a modification to the annual plan that does not put the transmission system at risk of an encroachment the annual plan may be modified. If 100 miles of the annual plan is deferred until next year the calculation to determine what percentage was completed for the current year would be: 1000 – 100 (deferred miles) = 900 modified annual plan, or 900 / 900 = 100% completed annual miles. If an applicable Transmission Owner or applicable Generator Owner only completed 875 of the total 1000 miles with no acceptable documentation for modification of the annual plan the calculation for failure to complete the annual plan would be: 1000 – 875 = 125 miles failed to complete then, 125 miles (not completed) / 1000 total annual plan miles = 12.5% failed to complete.

The ability to modify the work plan allows the applicable Transmission Owner or applicable Generator Owner to change priorities or treatment methodologies during the year as conditions or situations dictate. For example recent line inspections may identify unanticipated high priority work, weather conditions (drought) could make herbicide application ineffective during the plan year, or a major storm could require redirecting local resources away from planned maintenance. This situation may also include complying with mutual assistance agreements by moving resources off the applicable Transmission Owner's or applicable Generator Owner's system to work on another system. Any of these examples could result in acceptable deferrals or additions to the annual work plan provided that they do not put the transmission system at risk of a vegetation encroachment.
In general, the vegetation management maintenance approach should use the full extent of the applicable Transmission Owner's or applicable Generator Owner's easement, fee simple and other legal rights allowed. A comprehensive approach that exercises the full extent of legal rights on the ROW is superior to incremental management because in the long term it reduces the overall potential for encroachments, and it ensures that future planned work and future planned inspection cycles are sufficient.

When developing the annual work plan the applicable Transmission Owner or applicable Generator Owner should allow time for procedural requirements to obtain permits to work on federal, state, provincial, public, tribal lands. In some cases the lead time for obtaining permits may necessitate preparing work plans more than a year prior to work start dates. Applicable Transmission Owners or applicable Generator Owners may also need to consider those special landowner requirements as documented in easement instruments.

This requirement sets the expectation that the work identified in the annual work plan will be completed as planned. Therefore, deferrals or relevant changes to the annual plan shall be

documented. Depending on the planning and documentation format used by the applicable Transmission Owner or applicable Generator Owner, evidence of successful annual work plan execution could consist of signed-off work orders, signed contracts, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, or paid invoices. Other evidence may include photographs, and walk-through reports.

Notes:

The SDT determined that the use of IEEE 516-2003 in version 1 of FAC-003 was a misapplication. The SDT consulted specialists who advised that the Gallet equation would be a technically justified method. The explanation of why the Gallet approach is more appropriate is explained in the paragraphs below.

The drafting team sought a method of establishing minimum clearance distances that uses realistic weather conditions and realistic maximum transient over-voltages factors for in-service transmission lines.

The SDT considered several factors when looking at changes to the minimum vegetation to conductor distances in FAC-003-1:

- avoid the problem associated with referring to tables in another standard (IEEE-516-2003)
- transmission lines operate in non-laboratory environments (wet conditions)
- transient over-voltage factors are lower for in-service transmission lines than for inadvertently re-energized transmission lines with trapped charges.

FAC-003-1 used the minimum air insulation distance (MAID) without tools formula provided in IEEE 516-2003 to determine the minimum distance between a transmission line conductor and vegetation. The equations and methods provided in IEEE 516 were developed by an IEEE Task Force in 1968 from test data provided by thirteen independent laboratories. The distances provided in IEEE 516 Tables 5 and 7 are based on the withstand voltage of a dry rod-rod air gap, or in other words, dry laboratory conditions. Consequently, the validity of using these distances in an outside environment application has been questioned.

FAC-003-1 allowed Transmission Owners to use either Table 5 or Table 7 to establish the minimum clearance distances. Table 7 could be used if the Transmission Owner knew the maximum transient over-voltage factor for its system. Otherwise, Table 5 would have to be used. Table 5 represented minimum air insulation distances under the worst possible case for transient over-voltage factors. These worst case transient over-voltage factors were as follows: 3.5 for voltages up to 362 kV phase to phase; 3.0 for 500 - 550 kV phase to phase; and 2.5 for 765 to 800 kV phase to phase. These worst case over-voltage factors were also a cause for concern in this particular application of the distances.

In general, the worst case transient over-voltages occur on a transmission line that is inadvertently re-energized immediately after the line is de-energized and a trapped charge is

still present. The intent of FAC-003 is to keep a transmission line that is in service from becoming de-energized (i.e. tripped out) due to spark-over from the line conductor to nearby vegetation. Thus, the worst case transient overvoltage assumptions are not appropriate for this application. Rather, the appropriate over voltage values are those that occur only while the line is energized.

Typical values of transient over-voltages of in-service lines are not readily available in the literature because they are negligible compared with the maximums. A conservative value for the maximum transient over-voltage that can occur anywhere along the length of an in-service ac line was approximately 2.0 per unit. This value was a conservative estimate of the transient over-voltage that is created at the point of application (e.g. a substation) by switching a capacitor bank without pre-insertion devices (e.g. closing resistors). At voltage levels where capacitor banks are not very common (e.g. Maximum System Voltage of 362 kV), the maximum transient over-voltage of an in-service ac line are created by fault initiation on adjacent ac lines and shunt reactor bank switching. These transient voltages are usually 1.5 per unit or less.

Even though these transient over-voltages will not be experienced at locations remote from the bus at which they are created, in order to be conservative, it is assumed that all nearby ac lines are subjected to this same level of over-voltage. Thus, a maximum transient over-voltage factor of 2.0 per unit for transmission lines operated at 302 kV and below was considered to be a realistic maximum in this application. Likewise, for ac transmission lines operated at Maximum System Voltages of 362 kV and above a transient over-voltage factor of 1.4 per unit was considered a realistic maximum.

The Gallet equations are an accepted method for insulation coordination in tower design. These equations are used for computing the required strike distances for proper transmission line insulation coordination. They were developed for both wet and dry applications and can be used with any value of transient over-voltage factor. The Gallet equation also can take into account various air gap geometries. This approach was used to design the first 500 kV and 765 kV lines in North America.

If one compares the MAID using the IEEE 516-2003 Table 7 (table D.5 for English values) with the critical spark-over distances computed using the Gallet wet equations, for each of the nominal voltage classes and identical transient over-voltage factors, the Gallet equations yield a more conservative (larger) minimum distance value.

Distances calculated from either the IEEE 516 (dry) formulas or the Gallet “wet” formulas are not vastly different when the same transient overvoltage factors are used; the “wet” equations will consistently produce slightly larger distances than the IEEE 516 equations when the same transient overvoltage is used. While the IEEE 516 equations were only developed for dry conditions the Gallet equations have provisions to calculate spark-over distances for both wet and dry conditions.

Since no empirical data for spark over distances to live vegetation existed at the time version 3 was developed, the SDT chose a proven method that has been used in other EHV applications. The Gallet equations relevance to wet conditions and the selection of a Transient Overvoltage Factor that is consistent with the absence of trapped charges on an in-service transmission line make this methodology a better choice.

The following table is an example of the comparison of distances derived from IEEE 516 and the Gallet equations.

Comparison of spark-over distances computed using Gallet wet equations vs.

IEEE 516-2003 MAID distances

(AC) Nom System Voltage (kV)	**(AC) Max System Voltage (kV)**	**Transient Over-voltage Factor (T)**	**Clearance (ft.) Gallet (wet) @ Alt. 3000 feet**	Table 7 (Table D.5 for feet) **IEEE 516-2003 MAID (ft) @ Alt. 3000 feet**
765	800	2.0	14.36	13.95
500	550	2.4	11.0	10.07
345	362	3.0	8.55	7.47
230	242	3.0	5.28	4.2
115	121	3.0	2.46	2.1

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 Applicability (section 4.2.4):
The areas excluded in 4.2.4 were excluded based on comments from industry for reasons summarized as follows:

1) There is a very low risk from vegetation in this area. Based on an informal survey, no TOs reported such an event.
2) Substations, switchyards, and stations have many inspection and maintenance activities that are necessary for reliability. Those existing process manage the threat. As such, the formal steps in this standard are not well suited for this environment.
3) Specifically addressing the areas where the standard does and does not apply makes the standard clearer.

Rationale for Applicability (section 4.3):
Within the text of NERC Reliability Standard FAC-003-3, "transmission line(s)" and "applicable line(s)" can also refer to the generation Facilities as referenced in 4.3 and its subsections.

Rationale for R1 ~~and R2~~:
Lines with the highest significance to reliability are covered in R1; all other lines are covered in R2.

Rationale for the types of failure to manage vegetation which are listed in order of increasing degrees of severity in non-compliant performance as it relates to a failure of an applicable Transmission Owner's or applicable Generator Owner's vegetation maintenance program:

1. This management failure is found by routine inspection or Fault event investigation, and is normally symptomatic of unusual conditions in an otherwise sound program.
2. This management failure occurs when the height and location of a side tree within the ROW is not adequately addressed by the program.
3. This management failure occurs when side growth is not adequately addressed and may be indicative of an unsound program.
4. This management failure is usually indicative of a program that is not addressing the most fundamental dynamic of vegetation management, (i.e. a grow-in under the line). If this type of failure is pervasive on multiple lines, it provides a mechanism for a Cascade.

Rationale for R3:
The documentation provides a basis for evaluating the competency of the applicable Transmission Owner's or applicable Generator Owner's vegetation program. There may be many acceptable approaches to maintain clearances. Any approach must demonstrate that the

applicable Transmission Owner or applicable Generator Owner avoids vegetation-to-wire conflicts under all Ratings and all Rated Electrical Operating Conditions.

Rationale for R4:

This is to ensure expeditious communication between the applicable Transmission Owner or applicable Generator Owner and the control center when a critical situation is confirmed.

Rationale for R5:

Legal actions and other events may occur which result in constraints that prevent the applicable Transmission Owner or applicable Generator Owner from performing planned vegetation maintenance work.

In cases where the transmission line is put at potential risk due to constraints, the intent is for the applicable Transmission Owner and applicable Generator Owner to put interim measures in place, rather than do nothing.

The corrective action process is not intended to address situations where a planned work methodology cannot be performed but an alternate work methodology can be used.

Rationale for R6:

Inspections are used by applicable Transmission Owners and applicable Generator Owners to assess the condition of the entire ROW. The information from the assessment can be used to determine risk, determine future work and evaluate recently-completed work. This requirement sets a minimum Vegetation Inspection frequency of once per calendar year but with no more than 18 months between inspections on the same ROW. Based upon average growth rates across North America and on common utility practice, this minimum frequency is reasonable. Transmission Owners should consider local and environmental factors that could warrant more frequent inspections.

Rationale for R7:

This requirement sets the expectation that the work identified in the annual work plan will be completed as planned. It allows modifications to the planned work for changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors, provided that those modifications do not put the transmission system at risk of a vegetation encroachment.

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 initial ballot	09/29/17 – 11/14/17

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2018 – October 2018
10-day final ballot	October 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** System Operating Limits Methodology for the Operations Horizon

2. **Number:** FAC-011-4

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.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinator

5. **Effective Date:** See Implementation Plan for Project 2015-09.

B. Requirements and Measures

R1. Each Reliability Coordinator shall have a documented methodology for establishing SOLs (i.e., SOL Methodology) within its Reliability Coordinator Area. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology.

R2. Each Reliability Coordinator shall include in its SOL Methodology the method for Transmission Operators to determine which owner-provided Facility Ratings are to be used in operations such that the Transmission Operator and its Reliability Coordinator use common Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R2.

R3. Each Reliability Coordinator shall include in its SOL Methodology the method for Transmission Operators to determine the System Voltage Limits to be used in operations. The method shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

3.1. Require that each BES bus/station have an associated System Voltage Limit, unless the Reliability Coordinators SOL Methodology specifically allows the exclusion of BES buses/stations from the requirement to have an associated System Voltage Limit;

3.2. Require that System Voltage Limits respect voltage-based Facility Ratings;

3.3. Require that System Voltage Limits are greater than or equal to in-service relay settings for under voltage load shedding systems and Undervoltage Load Shedding Programs;

3.4. Identify the lowest allowable System Voltage Limit;

3.5. Require the use of common System Voltage Limits between the Transmission Operator and its Reliability Coordinator and provide the method for determining the common System Voltage Limits to be used in operations;

3.6. Address coordination of System Voltage Limits between adjacent Transmission Operators in its Reliability Coordinator Area; and

3.7. Address coordination of System Voltage Limits between adjacent Reliability Coordinator Areas within an Interconnection.

M3. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R3.

R4. Each Reliability Coordinator shall include in its SOL Methodology the method for determining the stability limits to be used in operations. The method shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1. Specify stability performance criteria, including any margins applied. The criteria shall, at a minimum, include the following:

4.1.1. steady-state voltage stability;

4.1.2. transient voltage response;

4.1.3. unit stability; and

4.1.4. System damping.

4.2. Require that stability limits are established to meet the criteria specified in Part 4.1 for the Contingencies identified in Requirement R5.

4.3. Describe how the Reliability Coordinator establishes stability limits when there is an impact to more than one Transmission Operator in its Reliability Coordinator Area.

4.4. Describe how stability limits are determined, considering levels of transfers, Load and generation dispatch, and System conditions including any changes to System topology such as Facility outages.

4.5. Describe the level of detail that is required for the study model(s), including the extent of the Reliability Coordinator Area, as well as the critical modeling details from other Reliability Coordinator Areas, necessary to determine different types of stability limits.

4.6. Describe the allowed uses of Remedial Action Schemes and other automatic post-Contingency mitigation actions in establishing stability limits used in operations.

4.7. State that the use of underfrequency load shedding (UFLS) programs and Undervoltage Load Shedding Programs are not allowed in the establishment of stability limits.

M4. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R4.

R5. Each Reliability Coordinator shall identify in its SOL Methodology the Contingency events for use in determining stability limits and performing Operational Planning Analysis (OPAs) and Real-time Assessments (RTAs) for the area under study. The SOL Methodology shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. Specify the following single Contingency events for use in determining stability limits and performing OPAs and RTAs:

5.1.1. Loss of any of the following either by single phase to ground or three phase Fault (whichever is more severe) with Normal Clearing, or without a Fault:

- generator;
- transmission circuit;
- transformer;
- shunt device; or
- single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

5.2. Identify any additional single or multiple Contingency events or types of Contingency events for use in performing Operational Planning Analysis and Real-time Assessments.

5.3. Identify any additional single or multiple Contingency events or types of Contingency events for use in determining stability limits.

5.4. Describe the method(s) for identifying which, if any, of the Contingency events provided by the Planning Coordinator or Transmission Planner in accordance with FAC-015-1, Requirement R4, to use in determining stability limits.

M5. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R5.

R6. Each Reliability Coordinator shall include in its SOL Methodology, at a minimum, the following Bulk Electric System performance criteria: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

6.1. The actual pre-Contingency state (Real-time monitoring and Real-time Assessment) and anticipated pre-Contingency state (Operational Planning Analysis) demonstrates the following:

6.1.1. Flow through Facilities are within Normal Ratings; however, Emergency Ratings may be used when System adjustments to return the flow within its Normal Rating could be executed and completed within the specified time duration of those Emergency Ratings.

6.1.2. Voltages are within normal System Voltage Limits; however, emergency System Voltage Limits may be used when System adjustments to return the voltage within its normal System Voltage Limits could be executed and completed within the specified time duration of those emergency System Voltage Limits.

6.1.3. Instability, Cascading or uncontrolled separation do not occur.

6.2. The evaluation of potential single Contingencies listed in Part 5.1.1 against the actual pre-Contingency state (Real-time monitoring and Real-time Assessments) and anticipated pre-Contingency state (Operational Planning Analysis) demonstrates the following:

6.2.1. Flow through Facilities are within applicable Emergency Ratings, provided that System adjustments could be executed and completed within the specified time duration of those Emergency Ratings. Flow through a Facility must not be above the Facility's highest Emergency Rating.

6.2.2. Voltages are within emergency System Voltage Limits.

6.2.3. Instability, Cascading or uncontrolled separation do not occur.

6.3. The evaluation of the potential Contingencies identified in Part 5.2 against the actual pre-Contingency state (Real-time monitoring and Real-time Assessments) and anticipated pre-Contingency state (Operational Planning Analysis) demonstrates that instability, Cascading, or uncontrolled separation does not occur.

6.4. The evaluation of the potential Contingencies identified in Part 5.3 demonstrates that instability does not occur.

6.5. In determining the System's response to any Contingency identified in Parts 5.1 through 5.3, planned load shedding is acceptable only after all other available System adjustments have been made.

M6. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R6.

R7. Each Reliability Coordinator shall include in its SOL Methodology: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

7.1. A description of how to identify the subset of SOLs that qualify as Interconnection Reliability Operating Limits (IROLs).

7.2. Criteria for determining when violating a SOL qualifies as an IROL and criteria for developing any associated IROL T_V.

M7. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R6.

R8. Each Reliability Coordinator shall include in its SOL Methodology the method for Transmission Operators to communicate their established SOLs to the Reliability Coordinator. The method shall address the periodicity for communicating established SOLs. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M8. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R7.

R9. Each Reliability Coordinator shall provide its SOL Methodology to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

9.1. Each Reliability Coordinator that requests and indicates it has a reliability-related need within 30 days of a request.

9.2. Each of the following entities prior to the effective date of the SOL methodology:

9.2.1. Each adjacent Reliability Coordinator within the same Interconnection;

9.2.2. Each Planning Coordinator and Transmission Planner that is responsible for planning any portion of the Reliability Coordinator Area;

9.2.3. Each Transmission Operator within its Reliability Coordinator Area; and

9.2.4. Each Reliability Coordinator that has requested to receive updates and indicated it had a reliability-related need.

M9. Acceptable evidence that the Reliability Coordinator provided its SOL Methodology to the entities identified in Requirement R8 may include, but is not limited to, dated electronic or hard copy documentation such as emails with receipts, registered mail receipts, or postings to a secure web site with accompanying notification(s).

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 shall keep data or evidence of compliance with Requirements R1 through R9 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 did not have a SOL Methodology for establishing SOLs within its Reliability Coordinator Area.
R2.	N/A	N/A	The Reliability Coordinator included in its SOL Methodology the method for Transmission Operators to determine the applicable owner-provided Facility Ratings to be used in operations, but the method did not address the use of common Facility Ratings between the Reliability Coordinator and the Transmission Operators in its Reliability Coordinator Area	The Reliability Coordinator did not include in its SOL Methodology the method for Transmission Operators to determine the applicable owner-provided Facility Ratings to be used in operations.
R3.	The Reliability Coordinator failed to incorporate one of the Parts of Requirement R3 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts of Requirement R3 into its SOL Methodology.	The Reliability Coordinator failed to incorporate three of the Parts of Requirement R3 into its SOL Methodology.	The Reliability Coordinator failed to incorporate four or more of the Parts of

				Requirement R3 into its SOL Methodology.
R4.	The Reliability Coordinator failed to incorporate one of the Parts of Requirement R4 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts of Requirement R4 into its SOL Methodology.	The Reliability Coordinator failed to incorporate three of the Parts of Requirement R4 into its SOL Methodology.	The Reliability Coordinator failed to incorporate four or more of the Parts of Requirement R4 into its SOL Methodology.
R5.	N/A	The Reliability Coordinator failed to incorporate one of the Parts 5.2, 5.3 or 5.4 of Requirement R5 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts 5.2, 5.3, or 5.4 of Requirement R5 into its SOL Methodology.	The Reliability Coordinator failed to incorporate Part 5.1 of Requirement R5 into its SOL Methodology. OR The Reliability Coordinator failed to incorporate Parts 5.2, 5.3, and 5.4 of Requirement R5 into its SOL Methodology.
R6.	The Reliability Coordinator failed to incorporate one of the Parts of Requirement R6 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts of Requirement R6 into its SOL Methodology.	The Reliability Coordinator failed to incorporate three of the Parts of Requirement R6 into its SOL Methodology.	The Reliability Coordinator failed to incorporate four of the Parts of Requirement R6 into its SOL Methodology.
R7.	N/A	N/A	The Reliability Coordinator failed to include Part 7.1 (a description of how to identify the subset of SOLs that qualify as IROLs) in its SOL Methodology.	The Reliability Coordinator failed to include Parts 7.1 and 7.2 in its SOL Methodology.

			OR The Reliability Coordinator failed to include Part 7.2 (a criteria for determining when violating a SOL qualifies as an IROL in its SOL Methodology. OR The Reliability Coordinator failed to include Part 7.2 (criteria for developing any associated IROL T_v) in its SOL Methodology.	
R8.	N/A	N/A	The Reliability Coordinator did not include in its SOL Methodology the periodicity of SOL communications for Transmission Operators to communicate SOLs the Transmission Operator established.	The Reliability Coordinator did not include in its SOL Methodology the method for Transmission Operators to communicate SOLs it established or the periodicity of SOL communication.
R9.	The Reliability Coordinator failed to provide its new or revised SOL Methodology to one of the parties specified in Requirement R9, Part 9.2 prior to the effective date OR	The Reliability Coordinator failed to provide its new or revised SOL Methodology to two of the parties specified in Requirement R9, Part 9.2 prior to the effective date OR	The Reliability Coordinator failed to provide its new or revised SOL Methodology to three of the parties specified in Requirement R9, Part 9.2 prior to the effective date OR	The Reliability Coordinator failed to provide its new or revised SOL Methodology to four or more of the parties specified in Requirement R9, Part 9.2 prior to the effective date

	The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part 9.1 but was late by less than or equal to 10 calendar days.	The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part 9.1, but was late by more than 10 calendar days but less than or equal to 20 calendar days.	The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part 9.1, but was late by more than 20 calendar days but less than or equal to 30 calendar days.	OR The Reliability Coordinator failed to provide its new or revised SOL Methodology to one or more of the parties specified in Requirement R9, Part 9.2 OR The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part 9.1, but was late by more than 30 calendar days. OR The Reliability Coordinator failed to provide its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part 9.1.

D. Regional Variances

None.

E. 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 October 1, 2008 Changed “Cascading Outage” to “Cascading” Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	February 7, 2013	R5 and associated elements approved by NERC Board for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
2	February 24, 2014	Updated VSLs based on June 24, 2013 approval.	
3	November 13, 2014	Adopted by the NERC Board	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
4		Project 2015-09 – Adopt revisions to standard.	Revisions

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 initial ballot	09/29/17 – 11/14/17

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2018 – October 2018
10-day final ballot	October 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** System Operating Limits Methodology for the Operations Horizon

2. **Number:** FAC-011-4

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.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinator

5. **Effective Date:** See Implementation Plan for Project 2015-09.

B. Requirements and Measures

R1. Each Reliability Coordinator shall have a documented methodology for establishing SOLs (i.e., SOL Methodology) within its Reliability Coordinator Area. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology.

R2. Each Reliability Coordinator shall include in its SOL Methodology the method for Transmission Operators to determine ~~the applicable~~which owner-provided Facility Ratings are to be used in operations~~. The method shall address the use of common Facility Ratings between the Reliability Coordinator and~~ such that the Transmission ~~Operators in~~Operator and its Reliability Coordinator ~~Area~~use common Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R2.

R3. Each Reliability Coordinator shall include in its SOL Methodology the method for Transmission Operators to determine the System Voltage Limits to be used in operations. The method shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

3.1. Require that each BES bus~~es~~/station~~s~~ have an associated System Voltage Limit, unless ~~except for~~ the Reliability Coordinators SOL Methodology specifically allows the exclusion of BES buses/stations ~~that may be excluded as specified in the Reliability Coordinator's SOL Methodology~~from the requirement to have an associated System Voltage Limit;

3.2. Require that System Voltage Limits respect ~~the~~voltage-based Facility ~~voltage~~ Ratings;

3.3. Require that System Voltage Limits are ~~higher~~greater than or equal to in-service relay settings for under voltage load shedding ~~(UVLS) relay settings~~systems and Undervoltage Load Shedding Programs;

3.4. Identify the lowest allowable System Voltage Limit;

3.5. ~~Address~~Require ~~-~~the use of common System Voltage Limits between the ~~Reliability Coordinator and the~~ Transmission ~~Operators in~~Operator and its Reliability Coordinator ~~Area~~ and provide the method for determining the common System Voltage Limits to be used in operations;

3.6. Address coordination of System Voltage Limits between adjacent Transmission Operators in its Reliability Coordinator Area; and

3.7. Address coordination of System Voltage Limits between adjacent Reliability Coordinator Areas within an Interconnection.

M3. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R3.

R4. Each Reliability Coordinator shall include in its SOL Methodology the method for determining the stability limits to be used in operations. The method shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1. Specify stability performance criteria, including any margins applied. The criteria shall, at a minimum, include the following:

4.1.1. steady-state voltage stability;

4.1.2. transient voltage response;

4.1.3. ~~angular~~unit stability; and

4.1.4. System damping.

4.2. Require that stability limits are established to meet the criteria specified in Part 4.1 for the Contingencies identified in Requirement R5.

4.3. Describe how the Reliability Coordinator establishes stability limits when there is an impact to more than one Transmission Operator in its Reliability Coordinator Area.

4.4. Describe how ~~instability risks~~stability limits are ~~identified~~determined, considering levels of transfers, Load and generation dispatch, and System conditions including any changes to System topology such as Facility outages~~;~~.

4.5. Describe the level of detail that is required for the study model(s)~~;~~, including the extent of the Reliability Coordinator Area, as well as the critical modeling details from other Reliability Coordinator Areas, necessary to determine different types of stability limits.

4.6. Describe the allowed uses of Remedial Action Schemes and other automatic post-Contingency mitigation actions in establishing stability limits used in operations. ~~;~~

~~4.6.~~4.7. State that the ~~planned~~ use of underfrequency load shedding (UFLS) ~~is~~programs and Undervoltage Load Shedding Programs are not allowed in the establishment of stability limits.

M4. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R4.

R5. Each Reliability Coordinator shall ~~include~~identify in its SOL Methodology the ~~method for identifying the single Contingencies and multiple Contingencies~~Contingency events for use in determining stability limits and performing Operational Planning Analysis (OPAs) and Real-time Assessments (RTAs~~).~~) for the area under study. The ~~method~~SOL Methodology shall ~~include~~: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. ~~The~~Specify the following ~~list of~~ single Contingency events for use in determining stability limits and performing OPAs and RTAs:

5.1.1. Loss of any of the following either by single phase to ground or three phase Fault (whichever is more severe) with ~~normal clearing~~Normal Clearing, or without a Fault:

- generator;
- transmission circuit;
- transformer;
- shunt device; or
- single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

5.2. ~~Any~~Identify any additional single or multiple Contingency events or types of ~~single~~ Contingency events ~~identified~~for use in performing Operational Planning Analysis and Real-time Assessments.

~~5.2.~~5.3. Identify any additional single or multiple Contingency events or types of Contingency events for use in determining stability limits~~, or for use in performing OPAs and RTAs.~~.

~~**5.3.** Any types of multiple Contingency events identified for use in determining stability limits, or for use in performing OPAs and RTAs.~~

5.4. ~~The method for considering~~Describe the method(s) for identifying which, if any, of the Contingency events provided by the Planning Coordinator or Transmission Planner in accordance with FAC-015-1, Requirement ~~R6 to identify the Contingencies for~~R4, to use in determining stability limits.

M5. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R5.

R6. Each Reliability Coordinator shall include in its SOL Methodology, at a minimum, the following Bulk Electric System performance criteria: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

6.1. The actual pre-Contingency state (Real-time monitoring and Real-time Assessment) and anticipated pre-Contingency state (Operational Planning Analysis) demonstrates the following:

6.1.1. Flow through Facilities are within Normal Ratings; however, Emergency Ratings may be used when System adjustments to return the flow within its Normal Rating could be executed and completed within the specified time duration of those Emergency Ratings.

6.1.2. Voltages are within normal System Voltage Limits; however, emergency System Voltage Limits may be used when System adjustments to return the voltage within its normal System Voltage Limits could be executed and completed within the specified time duration of those emergency System Voltage Limits.

6.1.3. Instability, Cascading or uncontrolled separation do not occur.

6.2. The evaluation of potential single Contingencies listed in Part 5.1.1 against the actual pre-Contingency state (Real-time monitoring and Real-time Assessments) and anticipated pre-Contingency state (Operational Planning Analysis) demonstrates the following:

6.2.1. Flow through Facilities are within applicable Emergency Ratings, provided that System adjustments could be executed and completed within the specified time duration of those Emergency Ratings. Flow through a Facility must not be above the Facility's highest Emergency Rating.

6.2.2. Voltages are within emergency System Voltage Limits.

6.2.3. Instability, Cascading or uncontrolled separation do not occur.

6.3. The evaluation of the potential Contingencies identified in Part 5.2 against the actual pre-Contingency state (Real-time monitoring and Real-time Assessments) and anticipated pre-Contingency state (Operational Planning Analysis) demonstrates that instability, Cascading, or uncontrolled separation does not occur.

6.4. The evaluation of the potential Contingencies identified in Part 5.3 demonstrates that instability does not occur.

6.5. In determining the System's response to any Contingency identified in Parts 5.1 through 5.3, planned load shedding is acceptable only after all other available System adjustments have been made.

M6. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R6.

~~R6.~~R7. Each Reliability Coordinator shall include in its SOL Methodology: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

~~6.1.~~7.1. A description of how to identify the subset of SOLs that qualify as Interconnection Reliability Operating Limits (IROLs).

~~6.2.~~7.2. Criteria for determining when violating a SOL qualifies as an IROL and criteria for developing any associated IROL T_v.

~~M6.~~M7. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R6.

~~R7.~~R8. Each Reliability Coordinator shall include in its SOL Methodology the method for Transmission Operators to communicate their established SOLs ~~it established~~ to the ~~its~~ Reliability Coordinator~~(s)~~. The method shall address the periodicity for communicating established~~of~~ SOLs~~ communication~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~M7.~~M8. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation of its SOL Methodology that addresses the items listed in Requirement R7.

~~R8.~~R9. Each Reliability Coordinator shall provide its SOL Methodology ~~and any changes to the SOL Methodology prior to the effective date of the SOL Methodology,~~ to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~8.1.~~9.1. Each~~Each adjacent Reliability Coordinator within an Interconnection,~~ ~~and each~~ Reliability Coordinator that requests and indicates it has a reliability-related need~~;~~ within 30 days of a request.

9.2. Each of the following entities prior to the effective date of the SOL methodology:

9.2.1. Each adjacent Reliability Coordinator within the same~~an~~ Interconnection;

~~8.1.1.~~9.2.2. Each Planning Coordinator and Transmission Planner that is responsible for planning any portion of the Reliability Coordinator Area;

~~8.1.2.~~9.2.3. Each Transmission Operator within its Reliability Coordinator Area~~.~~; and

9.2.4. Each Reliability Coordinator that has requested to receive updates and indicated it had a reliability-related need.

~~M8.~~M9. Acceptable evidence that the Reliability Coordinator provided its SOL Methodology to the entities identified in Requirement R8 may include, but is not limited to, dated electronic or hard copy documentation such as emails with receipts,

registered mail receipts, or postings to a secure web site with accompanying notification(s).

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 shall keep data or evidence of compliance with Requirements R1 through ~~R8~~R9 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 did not have a SOL Methodology for establishing SOLs within its Reliability Coordinator Area.
R2.	N/A	N/A	The Reliability Coordinator included in its SOL Methodology the method for Transmission Operators to determine the applicable owner-provided Facility Ratings to be used in operations, but the method did not address the use of common Facility Ratings between the Reliability Coordinator and the Transmission Operators in its Reliability Coordinator Area	The Reliability Coordinator did not include in its SOL Methodology the method for Transmission Operators to determine the applicable owner-provided Facility Ratings to be used in operations.
R3.	The Reliability Coordinator failed to incorporate one of the Parts of Requirement R3 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts of Requirement R3 into its SOL Methodology.	The Reliability Coordinator failed to incorporate three of the Parts of Requirement R3 into its SOL Methodology.	The Reliability Coordinator failed to incorporate four or more of the Parts of

				Requirement R3 into its SOL Methodology.
R4.	The Reliability Coordinator failed to incorporate one of the Parts of Requirement R4 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts of Requirement R4 into its SOL Methodology.	The Reliability Coordinator failed to incorporate three of the Parts of Requirement R4 into its SOL Methodology.	The Reliability Coordinator failed to incorporate four or more of the Parts of Requirement R4 into its SOL Methodology.
R5.	N/A	The Reliability Coordinator failed to incorporate one of the Parts 5.2, 5.3 or 5.4 of Requirement R5 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts 5.2, 5.3, or 5.4 of Requirement R5 into its SOL Methodology.	The Reliability Coordinator failed to incorporate Part 5.1 of Requirement R5 into its SOL Methodology. OR The Reliability Coordinator failed to incorporate Parts 5.2, 5.3, and 5.4 of Requirement R5 into its SOL Methodology.
R6.	The Reliability Coordinator failed to incorporate one of the Parts of Requirement R6 into its SOL Methodology.	The Reliability Coordinator failed to incorporate two of the Parts of Requirement R6 into its SOL Methodology.	The Reliability Coordinator failed to incorporate three of the Parts of Requirement R6 into its SOL Methodology.	The Reliability Coordinator failed to incorporate four of the Parts of Requirement R6 into its SOL Methodology.
~~R6~~R7.	N/A	N/A	The Reliability Coordinator failed to include Part ~~6~~7.1 (a description of how to identify the subset of SOLs that qualify as IROLs) in its SOL Methodology.	The Reliability Coordinator failed to include Parts ~~6~~7.1 and ~~6~~7.2 in its SOL Methodology.

			OR The Reliability Coordinator failed to include Part ~~6~~7.2 (a criteria for determining when violating a SOL qualifies as an IROL in its SOL Methodology. OR The Reliability Coordinator failed to include Part ~~6~~7.2 (criteria for developing any associated IROL T_v) in its SOL Methodology.	
~~**R7**~~**R8.**	N/A	N/A	The Reliability Coordinator did not include in its SOL Methodology the periodicity of SOL communications for Transmission Operators to communicate SOLs the Transmission Operator established.	The Reliability Coordinator did not include in its SOL Methodology the method for Transmission Operators to communicate SOLs it established or the periodicity of SOL communication.
~~**R8**~~**R9.**	The Reliability Coordinator failed to provide its new or revised SOL Methodology to one of the parties specified in Requirement R9, Part 9.2 prior to the effective date OR	The Reliability Coordinator failed to provide its new or revised SOL Methodology to two of the parties specified in Requirement R9, Part 9.2 prior to the effective date OR	The Reliability Coordinator failed to provide its new or revised SOL Methodology to ~~one~~three of the parties specified in ~~Parts 8.1 through 8.3.~~Requirement	The Reliability Coordinator failed to provide its new or revised SOL Methodology to ~~two~~four or more of the parties specified in ~~Parts 8.1 through 8.3.~~Requirement

	The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part ~~8.4~~9.1 but was late by less than or equal to 10 calendar days.	The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part ~~8.4~~9.1, but was late by more than 10 calendar days but less than or equal to 20 calendar days.	R9, Part 9.2 prior to the effective date OR The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part ~~8.4~~9.1, but was late by more than 20 calendar days but less than or equal to 30 calendar days.	R9, Part 9.2 prior to the effective date OR The Reliability Coordinator failed to provide its new or revised SOL Methodology to one or more of the parties specified in ~~Parts 8.1 through 8.3 prior to the effective date of the SOL Methodology.~~Requirement R9, Part 9.2 OR The Reliability Coordinator provided its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part ~~8.4~~9.1, but was late by more than 30 calendar days. OR The Reliability Coordinator failed to provide its new or revised SOL Methodology to a requesting Reliability Coordinator in accordance with Requirement R9, Part ~~8.4~~9.1.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board ~~of Trustees~~	New
2		Changed the effective date to October 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board ~~of Trustees~~: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	February 7, 2013	R5 and associated elements approved by NERC Board ~~of Trustees~~ for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
2	February 24, 2014	Updated VSLs based on June 24, 2013 approval.	
3	November 13, 2014	Adopted by the NERC Board ~~of Trustees~~	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
4		Project 2015-09 – Adopt revisions to standard.	Revisions

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

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

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

2. **Number:** FAC-013-3

3. **Purpose:** To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.

4. **Applicability:**

   4.1. Planning Coordinators

5. **Effective Date:**

See Implementation Plan for FAC-013-3.

B. Requirements and Measures

R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Criteria for the selection of the transfers to be assessed.

1.2. Reserved for future use.

1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's Planning Assessments.

1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:

1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.

1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.

1.4.3. System demand.

1.4.4. Current approved and projected Transmission uses.

1.4.5. Parallel path (loop flow) adjustments.

1.4.6. Contingencies

1.4.7. Monitored Facilities.

1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.

M1. Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.

R2. Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. Distribute to the following prior to the effectiveness of such revisions:

2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.

2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.

2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.

M2. Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]* (Retirement approved by FERC effective January 21, 2014.)

M3. Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. (Retirement approved by FERC effective January 21, 2014.)

R4. During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.

R5. Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M5. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5

R6. If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M6. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

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 Planning Coordinator 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 Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. (R3 retired-Retirement approved by FERC effective January 21, 2014.)
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

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

1.3. Compliance Monitoring and Enforcement 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.
Complaints

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.
R3. (Retirement approved by FERC effective	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
January 21, 2013.)	R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.
R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.
R5.	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requested data as required in Requirement R6.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	08/01/05	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Lower cased the word "draft" and "drafting team" where appropriate. 3. Changed Anticipated Action #5, page 1, from "30-day" to "Thirty-day." Added or removed "periods."	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	05/17/12	FERC Order issued directing the VRF's for Requirements R1. and R4. be changed from "Lower" to "Medium." FERC Order issued correcting the High and Severe VSL language for R1.	
2	02/7/13	R3 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	11/21/13	R3 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

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 adoption, the text from the rationale text boxes was moved to this section.

Rationale for R1:
Text, text, text

Rationale for R2:
Text, text, text

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

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

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

2. **Number:** FAC-013-32

3. **Purpose:** To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.

4. **Applicability:**

   4.1. Planning Coordinators

5. **Effective Date:**

See Implementation Plan for FAC-013-3.

B. Requirements and Measures

R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Criteria for the selection of the transfers to be assessed.

1.2. Reserved for future use~~A statement that the assessment shall respect known System Operating Limits (SOLs)~~.

1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's Planning~~planning~~ Assessments~~practices~~.

1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:

1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.

1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.

1.4.3. System demand.

1.4.4. Current approved and projected Transmission uses.

1.4.5. Parallel path (loop flow) adjustments.

1.4.6. Contingencies

1.4.7. Monitored Facilities.

1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.

M1. Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.

R2. Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. Distribute to the following prior to the effectiveness of such revisions:

2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.

2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.

2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.

M2. Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]* (Retirement approved by FERC effective January 21, 2014.)

M3. Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. (Retirement approved by FERC effective January 21, 2014.)

R4. During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.

R5. Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M5. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5

R6. If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M6. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

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 Planning Coordinator 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 Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. (R3 retired-Retirement approved by FERC effective January 21, 2014.)
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

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

1.3. Compliance Monitoring and Enforcement 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.
Complaints

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology: • Part 1.1 • ~~Part 1.2~~ • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology: • Part 1.1 • ~~Part 1.2~~ • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • ~~Part 1.2~~ • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.
R3. (Retirement approved by FERC effective	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
January 21, 2013.)	R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.
R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.
R5.	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requested data as required in Requirement R6.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	08/01/05	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Lower cased the word "draft" and "drafting team" where appropriate. 3. Changed Anticipated Action #5, page 1, from "30-day" to "Thirty-day." Added or removed "periods."	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	05/17/12	FERC Order issued directing the VRF's for Requirements R1. and R4. be changed from "Lower" to "Medium." FERC Order issued correcting the High and Severe VSL language for R1.	
2	02/7/13	R3 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	11/21/13	R3 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

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 adoption, the text from the rationale text boxes was moved to this section.

Rationale for R1:
Text, text, text

Rationale for R2:
Text, text, text

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

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2018 – October 2018
10-day final ballot	October 2018
NERC Board adoption	November 2018

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.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Reliability Coordinator
     - **4.1.2.** Transmission Operator
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 it 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. The Transmission Operator shall provide its SOLs to its Reliability Coordinator in accordance with its Reliability Coordinator's SOL Methodology. *[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 to be used in operations when the limit impacts 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 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 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 stability limit or IROL;

5.2.3 The associated IROL T_v for any IROL;

5.2.4 The associated Contingency(ies);

5.2.5 A description of the associated system conditions; 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 – 5.2.5 for each established stability limit or each 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.

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.

R6. Each Transmission Operator and Reliability Coordinator shall use the Bulk Electric System performance criteria specified in the Reliability Coordinator's SOL Methodology when performing OPAs, RTAs, and Real-time monitoring to determine SOL exceedances. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

M6. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation, that demonstrates the Transmission Operator and Reliability Coordinator used the Bulk Electric System performance criteria specified in the Reliability Coordinator's SOL methodology when performing OPAs, RTAs and Real-Time Monitoring.

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 or Transmission Operator 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 RC needs such information	The Transmission Operator failed to provide its SOLs to its Reliability Coordinator.

			to perform its reliability functions.	
R4.	N/A	N/A	N/A	The Reliability Coordinator failed to determine stability limits to be used in operations when the limit impacts 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 5.6.	The Reliability Coordinator failed to provide two of the items listed in Requirement R5, Parts 5.1 through 5.6.	The Reliability Coordinator failed to provide three of the items listed in Requirement R5, Parts 5.1 through 5.6.	The Reliability Coordinator failed to provide four or more of the items listed in Requirement R5, Parts 5.1 through 5.6.
R6.	N/A	N/A	N/A	A Transmission Operator or Reliability Coordinator failed to use the Bulk Electric System performance criteria specified in the Reliability Coordinator's SOL Methodology.

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
3		Project 2015-09 Adopt revised standard.	Revision

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

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~September 2017 – October 2017~~
45-day formal comment period with additional ballot	~~January~~August 2018 – ~~February~~October 2018
10-day final ballot	~~February~~October 2018
NERC Board ~~(Board)~~ adoption	~~May~~November 2018

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.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinator

   4.1.2. Transmission Operator

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 ~~to demonstrate~~ that demonstrates the Reliability Coordinator established IROLs in accordance with it 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 ~~to demonstrate~~ that demonstrates the Transmission Operator established SOLs in accordance with its Reliability Coordinator's SOL Methodology.

R3. The Transmission Operator shall provide its SOLs to its Reliability Coordinator in accordance with its Reliability Coordinator's SOL Methodology. *[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 ~~to demonstrate~~ 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 to be used in operations when the limit impacts 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 ~~to demonstrate~~ 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 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 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 IROL;

5.2.3 The associated IROL T_v for any IROL;

5.2.4 The associated Contingency(ies);

5.2.5 A description of the associated system conditions; 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 – 5.2.5 for each established stability limit or each 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.

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

R6. Each Transmission Operator and Reliability Coordinator ~~that is impacted by an IROL~~ shall ~~provide Transmission Owners and Generation Owners within its~~ use the Bulk Electric System performance criteria specified in the Reliability ~~Coordinator Area a list of Facilities owned by that entity that are critical~~Coordinator's SOL Methodology when performing OPAs, RTAs, and Real-time monitoring to ~~the derivation of the IROL.~~determine SOL exceedances. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

M6. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation ~~to demonstrate~~, that demonstrates the Transmission Operator and Reliability Coordinator ~~provided~~used the ~~list of Facilities~~Bulk Electric System performance criteria specified in ~~accordance with Requirement R6~~the Reliability Coordinator's SOL methodology when performing OPAs, RTAs and Real-Time Monitoring.

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 or Transmission Operator shall keep data or evidence of Requirements R1 through ~~R6~~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 ~~did not~~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 ~~did not~~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 ~~did not~~failed to provide its SOLs at the periodicity at which the RC needs such	The Transmission Operator ~~did not~~failed to provide its SOLs to its Reliability Coordinator.

			information to perform its reliability functions.	
R4.	N/A	N/A	N/A	The Reliability Coordinator ~~did not~~failed to determine stability limits to be used in operations when the limit impacts more than one Transmission Operator in its Reliability Coordinator Area in accordance with its SOL Methodology.
R5.	The Reliability Coordinator ~~did not~~failed to provide one of the items listed in Requirement R5, Parts 5.1 through 5.~~5~~6.	The Reliability Coordinator ~~did not~~failed to provide two of the items listed in Requirement R5, Parts 5.1 through 5.~~5~~6.	The Reliability Coordinator ~~did not~~failed to provide three of the items listed in Requirement R5, Parts 5.1 through 5.~~5~~6.	The Reliability Coordinator ~~did not~~failed to provide four or more of the items listed in Requirement R5, Parts 5.1 through 5.~~5~~6.
R6.	N/A	N/A	N/A	~~The Reliability Coordinator with an established IROL, or the Reliability Coordinator impacted by a neighboring Reliability Coordinator IROL, did not provide Transmission Owners or Generation Owners within its Reliability Coordinator Area a list of Facilities owned by that entity that are critical to the derivation of the IROL.~~A Transmission Operator or

				Reliability Coordinator failed to use the Bulk Electric System performance criteria specified in the Reliability Coordinator's SOL Methodology.

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 ~~of Trustees~~	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 ~~of Trustees~~: 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
3		Project 2015-09 Adopt revised standard.	Revision

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 Board of Trustees.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** Disturbance Monitoring and Reporting Requirements

2. **Number:** PRC-002-3

3. **Purpose:** To have adequate data available to facilitate analysis of Bulk Electric System (BES) Disturbances.

4. **Applicability:**

   Functional Entities:

   4.1 Reliability Coordinator

   4.2 Transmission Owner

   4.3 Generator Owner

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

B. Requirements and Measures

R1. Each Transmission Owner shall: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. Identify BES buses for which sequence of events recording (SER) and fault recording (FR) data is required by using the methodology in PRC-002-2, Attachment 1.

1.2. Notify other owners of BES Elements connected to those BES buses, if any, within 90-calendar days of completion of Part 1.1, that those BES Elements require SER data and/or FR data.

1.3. Re-evaluate all BES buses at least once every five calendar years in accordance with Part 1.1 and notify other owners, if any, in accordance with Part 1.2, and implement the re-evaluated list of BES buses as per the Implementation Plan.

M1. The Transmission Owner has a dated (electronic or hard copy) list of BES buses for which SER and FR data is required, identified in accordance with PRC-002-2, Attachment 1, and evidence that all BES buses have been re-evaluated within the required intervals under Requirement R1. The Transmission Owner will also have dated (electronic or hard copy) evidence that it notified other owners in accordance with Requirement R1.

R2. Each Transmission Owner and Generator Owner shall have SER data for circuit breaker position (open/close) for each circuit breaker it owns connected directly to the BES buses identified in Requirement R1 and associated with the BES Elements at those BES buses. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of SER data for circuit breaker position as specified in Requirement R2. Evidence may include, but is not limited to: (1) documents describing the device interconnections and configurations which may include a single design standard as representative for common installations; or (2) actual data recordings; or (3) station drawings.

R3. Each Transmission Owner and Generator Owner shall have FR data to determine the following electrical quantities for each triggered FR for the BES Elements it owns connected to the BES buses identified in Requirement R1: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1 Phase-to-neutral voltage for each phase of each specified BES bus.

3.2 Each phase current and the residual or neutral current for the following BES Elements:

3.2.1 Transformers that have a low-side operating voltage of 100kV or above.

3.2.2 Transmission Lines.

M3. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of FR data that is sufficient to determine electrical quantities as specified in Requirement R3. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations which may include a single design standard as representative for common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R4. Each Transmission Owner and Generator Owner shall have FR data as specified in Requirement R3 that meets the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

4.1 A single record or multiple records that include:

- A pre-trigger record length of at least two cycles and a total record length of at least 30-cycles for the same trigger point, or
- At least two cycles of the pre-trigger data, the first three cycles of the post-trigger data, and the final cycle of the fault as seen by the fault recorder.

4.2 A minimum recording rate of 16 samples per cycle.

4.3 Trigger settings for at least the following:

4.3.1 Neutral (residual) overcurrent.

4.3.2 Phase undervoltage or overcurrent.

M4. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that FR data meets Requirement R4. Evidence may include, but is not limited to: (1) documents describing the device specification (R4, Part 4.2) and device configuration or settings (R4, Parts 4.1 and 4.3), or (2) actual data recordings or derivations.

R5. Each Reliability Coordinator shall: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

5.1 Identify BES Elements for which dynamic Disturbance recording (DDR) data is required, including the following:

5.1.1 Generating resource(s) with:

5.1.1.1 Gross individual nameplate rating greater than or equal to 500 MVA.

5.1.1.2 Gross individual nameplate rating greater than or equal to 300 MVA where the gross plant/facility aggregate nameplate rating is greater than or equal to 1,000 MVA.

5.1.2 Any one BES Element that is part of a stability (angular or voltage) related System Operating Limit (SOL).

5.1.3 Each terminal of a high voltage direct current (HVDC) circuit with a nameplate rating greater than or equal to 300 MVA, on the alternating current (AC) portion of the converter.

5.1.4 One or more BES Elements that are part of an Interconnection Reliability Operating Limit (IROL).

5.1.5 Any one BES Element within a major voltage sensitive area as defined by an area with an in-service undervoltage load shedding (UVLS) program.

5.2 Identify a minimum DDR coverage, inclusive of those BES Elements identified in Part 5.1, of at least:

5.2.1 One BES Element; and

5.2.2 One BES Element per 3,000 MW of the Reliability Coordinator's historical simultaneous peak System Demand.

5.3 Notify all owners of identified BES Elements, within 90-calendar days of completion of Part 5.1, that their respective BES Elements require DDR data when requested.

5.4 Re-evaluate all BES Elements at least once every five calendar years in accordance with Parts 5.1 and 5.2, and notify owners in accordance with Part 5.3 to implement the re-evaluated list of BES Elements as per the Implementation Plan.

M5. The Reliability Coordinator has a dated (electronic or hard copy) list of BES Elements for which DDR data is required, developed in accordance with Requirement R5, Part 5.1 and Part 5.2; and re-evaluated in accordance with Part 5.4. The Reliability Coordinator has dated evidence (electronic or hard copy) that each Transmission Owner or Generator Owner has been notified in accordance with Requirement 5, Part 5.3. Evidence may include, but is not limited to: letters, emails, electronic files, or hard copy records demonstrating transmittal of information.

R6. Each Transmission Owner shall have DDR data to determine the following electrical quantities for each BES Element it owns for which it received notification as identified in Requirement R5: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

6.1 One phase-to-neutral or positive sequence voltage.

6.2 The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R6, Part 6.1, or the positive sequence current.

6.3 Real Power and Reactive Power flows expressed on a three phase basis corresponding to all circuits where current measurements are required.

6.4 Frequency of any one of the voltage(s) in Requirement R6, Part 6.1.

M6. The Transmission Owner has evidence (electronic or hard copy) of DDR data to determine electrical quantities as specified in Requirement R6. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R7. Each Generator Owner shall have DDR data to determine the following electrical quantities for each BES Element it owns for which it received notification as identified in Requirement R5: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

7.1 One phase-to-neutral, phase-to-phase, or positive sequence voltage at either the generator step-up transformer (GSU) high-side or low-side voltage level.

7.2 The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R7, Part 7.1, phase current(s) for any phase-to-phase voltages, or positive sequence current.

7.3 Real Power and Reactive Power flows expressed on a three phase basis corresponding to all circuits where current measurements are required.

7.4 Frequency of at least one of the voltages in Requirement R7, Part 7.1.

M7. The Generator Owner has evidence (electronic or hard copy) of DDR data to determine electrical quantities as specified in Requirement R7. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R8. Each Transmission Owner and Generator Owner responsible for DDR data for the BES Elements identified in Requirement R5 shall have continuous data recording and storage. If the equipment was installed prior to the effective date of this standard and is not capable of continuous recording, triggered records must meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

8.1 Triggered record lengths of at least three minutes.

8.2 At least one of the following three triggers:

- Off nominal frequency trigger set at:

	Low	High
○ Eastern Interconnection	<59.75 Hz	>61.0 Hz
○ Western Interconnection	<59.55 Hz	>61.0 Hz
○ ERCOT Interconnection	<59.35 Hz	>61.0 Hz
○ Hydro-Quebec Interconnection	<58.55 Hz	>61.5 Hz

- Rate of change of frequency trigger set at:

○ Eastern Interconnection	< -0.03125 Hz/sec	> 0.125 Hz/sec
○ Western Interconnection	< -0.05625 Hz/sec	> 0.125 Hz/sec
○ ERCOT Interconnection	< -0.08125 Hz/sec	> 0.125 Hz/sec
○ Hydro-Quebec Interconnection	< -0.18125 Hz/sec	> 0.1875 Hz/sec

- Undervoltage trigger set no lower than 85 percent of normal operating voltage for a duration of 5 seconds.

M8. Each Transmission Owner and Generator Owner has dated evidence (electronic or hard copy) of data recordings and storage in accordance with Requirement R8. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (2) actual data recordings.

R9. Each Transmission Owner and Generator Owner responsible for DDR data for the BES Elements identified in Requirement R5 shall have DDR data that meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

9.1 Input sampling rate of at least 960 samples per second.

9.2 Output recording rate of electrical quantities of at least 30 times per second.

M9. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that DDR data meets Requirement R9. Evidence may include, but is not limited to: (1) documents describing the device specification, device configuration, or settings (R9, Part 9.1; R9, Part 9.2); or (2) actual data recordings (R9, Part 9.2).

R10. Each Transmission Owner and Generator Owner shall time synchronize all SER and FR data for the BES buses identified in Requirement R1 and DDR data for the BES

Elements identified in Requirement R5 to meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

10.1 Synchronization to Coordinated Universal Time (UTC) with or without a local time offset.

10.2 Synchronized device clock accuracy within ± 2 milliseconds of UTC.

M10. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of time synchronization described in Requirement R10. Evidence may include, but is not limited to: (1) documents describing the device specification, configuration, or setting; (2) time synchronization indication or status; or 3) station drawings.

R11. Each Transmission Owner and Generator Owner shall provide, upon request, all SER and FR data for the BES buses identified in Requirement R1 and DDR data for the BES Elements identified in Requirement R5 to the Reliability Coordinator, Regional Entity, or NERC in accordance with the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

11.1 Data will be retrievable for the period of 10-calendar days, inclusive of the day the data was recorded.

11.2 Data subject to Part 11.1 will be provided within 30-calendar days of a request unless an extension is granted by the requestor.

11.3 SER data will be provided in ASCII Comma Separated Value (CSV) format following Attachment 2.

11.4 FR and DDR data will be provided in electronic files that are formatted in conformance with C37.111, (IEEE Standard for Common Format for Transient Data Exchange (COMTRADE), revision C37.111-1999 or later.

11.5 Data files will be named in conformance with C37.232, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME), revision C37.232-2011 or later.

M11. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that data was submitted upon request in accordance with Requirement R11. Evidence may include, but is not limited to: (1) dated transmittals to the requesting entity with formatted records; (2) documents describing data storage capability, device specification, configuration or settings; or (3) actual data recordings.

R12. Each Transmission Owner and Generator Owner shall, within 90-calendar days of the discovery of a failure of the recording capability for the SER, FR or DDR data, either: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- Restore the recording capability, or
- Submit a Corrective Action Plan (CAP) to the Regional Entity and implement it.

M12. The Transmission Owner or Generator Owner has dated evidence (electronic or hard copy) that meets Requirement R12. Evidence may include, but is not limited to: (1) dated reports of discovery of a failure, (2) documentation noting the date the data recording was restored, (3) SCADA records, or (4) dated CAP transmittals to the Regional Entity and evidence that it implemented the CAP.

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 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 Transmission Owner, Generator Owner, and Reliability Coordinator 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 Owner shall retain evidence of Requirement R1, Measure M1 for five calendar years.

The Transmission Owner shall retain evidence of Requirement R6, Measure M6 for three calendar years.

The Generator Owner shall retain evidence of Requirement R7, Measure M7 for three calendar years.

The Transmission Owner and Generator Owner shall retain evidence of requested data provided as per Requirements R2, R3, R4, R8, R9, R10, R11, and R12, Measures M2, M3, M4, M8, M9, M10, M11, and M12 for three calendar years.

The Reliability Coordinator shall retain evidence of Requirement R5, Measure M5 for five calendar years.

If a Transmission Owner, Generator Owner, or Reliability Coordinator is found non-compliant, it shall keep information related to the non-compliance until mitigation is completed and approved or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Lower	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 80 percent but less than 100 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by 30-calendar days or less. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying the other	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 70 percent but less than or equal to 80 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by greater than 30-calendar days and less than or equal to 60-calendar days. OR The Transmission Owner as directed by Requirement R1, Part	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 60 percent but less than or equal to 70 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by greater than 60-calendar days and less than or equal to 90-calendar days. OR The Transmission Owner as directed by Requirement R1, Part	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for less than or equal to 60 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by greater than 90-calendar days. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying one or more other owners by

			owners by 10-calendar days or less.	1.2 was late in notifying the other owners by greater than 10-calendar days but less than or equal to 20-calendar days.	1.2 was late in notifying the other owners by greater than 20-calendar days but less than or equal to 30-calendar days.	greater than 30-calendar days.
R2	Long-term Planning	Lower	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 80 percent but less than 100 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 70 percent but less than or equal to 80 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 60 percent but less than or equal to 70 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 for less than or equal to 60 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.
R3	Long-term Planning	Lower	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 80 percent but less than 100 percent of the total set of required electrical	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 70 percent but less than or equal to 80 percent of the total set of required	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 60 percent but less than or equal to 70 percent of the total set of required	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers less than or equal to 60 percent of the total set of required electrical quantities,

			quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.	electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.	electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.	which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.
R4	Long-term Planning	Lower	The Transmission Owner or Generator Owner had FR data that meets more than 80 percent but less than 100 percent of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 70 percent but less than or equal to 80 percent of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 60 percent but less than or equal to 70 percent of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets less than or equal to 60 percent of the total recording properties as specified in Requirement R4.
R5	Long-term Planning	Lower	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 80 percent but less than 100 percent of the required BES Elements included in Part 5.1.	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 70 percent but less than or equal to 80 percent of the required BES Elements included in Part 5.1.	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 60 percent but less than or equal to 70 percent of the required BES Elements included in Part 5.1.	The Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for less than or equal to 60 percent of the required BES Elements included in Part 5.1. OR

			OR The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by 30-calendar days or less. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners by 10-calendar days or less.	OR The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by greater than 30-calendar days and less than or equal to 60 -calendar days. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners by greater than 10-calendar days but less than or equal to 20-calendar days.	OR The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by greater than 60-calendar days and less than or equal to 90-calendar days. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners by greater than 20-calendar days but less than or equal to 30-calendar days.	The Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by greater than 90-calendar days. OR The Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying one or more owners by greater than 30-calendar days. OR The Reliability Coordinator failed to ensure a minimum DDR coverage per Part 5.2.
R6	Long-term Planning	Lower	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 that covered more than 80	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 70 percent	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 60 percent	The Transmission Owner failed to have DDR data as directed by Requirement R6, Parts 6.1 through 6.4.

			percent but less than 100 percent of the total required electrical quantities for all applicable BES Elements.	but less than or equal to 80 percent of the total required electrical quantities for all applicable BES Elements.	but less than or equal to 70 percent of the total required electrical quantities for all applicable BES Elements.	
R7	Long-term Planning	Lower	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 that covers more than 80 percent but less than 100 percent of the total required electrical quantities for all applicable BES Elements.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 70 percent but less than or equal to 80 percent of the total required electrical quantities for all applicable BES Elements.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 60 percent but less than or equal to 70 percent of the total required electrical quantities for all applicable BES Elements.	The Generator Owner failed to have DDR data as directed by Requirement R7, Parts 7.1 through 7.4.
R8	Long-term Planning	Lower	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 80 percent but less than 100 percent of the BES Elements they own as	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 70 percent but less than or equal to 80 percent of the BES Elements they	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 60 percent but less than or equal to 70 percent of the BES Elements they	The Transmission Owner or Generator Owner failed to have continuous or non-continuous DDR data, as directed in Requirement R8, for the BES Elements they own as determined in Requirement R5.

			determined in Requirement R5.	own as determined in Requirement R5.	own as determined in Requirement R5.	
R9	Long-term Planning	Lower	The Transmission Owner or Generator Owner had DDR data that meets more than 80 percent but less than 100 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets more than 70 percent but less than or equal to 80 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets more than 60 percent but less than or equal to 70 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets less than or equal to 60 percent of the total recording properties as specified in Requirement R9.
R10	Long-term Planning	Lower	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more than 90 percent but less than 100 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more than 80 percent but less than or equal to 90 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more than 70 percent but less than or equal to 80 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as	The Transmission Owner or Generator Owner failed to have time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for less than or equal to 70 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.

				directed by Requirement R10.	directed by Requirement R10.	
R11	Long-term Planning	Lower	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 30-calendar days but less than 40-calendar days after the request unless an extension was granted by the requesting authority. OR The Transmission Owner or Generator	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 40-calendar days but less than or equal to 50-calendar days after the request unless an extension was granted by the requesting authority. OR The Transmission Owner or Generator	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 50-calendar days but less than or equal to 60-calendar days after the request unless an extension was granted by the requesting authority. OR The Transmission Owner or Generator	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 failed to provide the requested data more than 60-calendar days after the request unless an extension was granted by the requesting authority. OR The Transmission Owner or Generator Owner as directed by Requirement R11

			Owner as directed by Requirement R11 provided more than 90 percent but less than 100 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 90 percent of the data but less than 100 percent of the data in the proper data format.	Owner as directed by Requirement R11 provided more than 80 percent but less than or equal to 90 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 80 percent of the data but less than or equal to 90 percent of the data in the proper data format.	Owner as directed by Requirement R11 provided more than 70 percent but less than or equal to 80 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 70 percent of the data but less than or equal to 80 percent of the data in the proper data format.	failed to provide less than or equal to 70 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided less than or equal to 70 percent of the data in the proper data format.
R12	Long-term Planning	Lower	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 90-calendar days but less than or equal	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 100-calendar days but less than or	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 110-calendar days but less than or	The Transmission Owner or Generator Owner as directed by Requirement R12 failed to report a failure and provide a Corrective Action Plan to the Regional Entity more than 120-calendar days after

			to 100-calendar days after discovery of the failure.	equal to 110-calendar days after discovery of the failure.	equal to 120-calendar days after discovery of the failure. OR The Transmission Owner or Generator Owner as directed by Requirement R12 submitted a CAP to the Regional Entity but failed to implement it.	discovery of the failure. OR Transmission Owner or Generator Owner as directed by Requirement R12 failed to restore the recording capability and failed to submit a CAP to the Regional Entity.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

G. References

IEEE C37.111: Common format for transient data exchange (COMTRADE) for power Systems.

IEEE C37.232-2011, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME). Standard published 11/09/2011 by IEEE.

NPCC SP6 Report Synchronized Event Data Reporting, revised March 31, 2005

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

U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout in the United States and Canada (Nov. 2003)

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
1	August 2, 2006	Adopted by NERC Board of Trustees	Revised
2	November 13, 2014	Adopted by NERC Board of Trustees	Revised under Project 2007-11 and merged with PRC-018-1.
2	September 24, 2015	FERC approved PRC-005-4. Docket No. RM15-4-000; Order No. 814	

Attachment 1

Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data

(Requirement R1)

To identify monitored BES buses for sequence of events recording (SER) and Fault recording (FR) data required by Requirement 1, each Transmission Owner shall follow sequentially, unless otherwise noted, the steps listed below:

Step 1. Determine a complete list of BES buses that it owns.

For the purposes of this standard, a single BES bus includes physical buses with breakers connected at the same voltage level within the same physical location sharing a common ground grid. These buses may be modeled or represented by a single node in fault studies. For example, ring bus or breaker-and-a-half bus configurations are considered to be a single bus.

Step 2. Reduce the list to those BES buses that have a maximum available calculated three phase short circuit MVA of 1,500 MVA or greater. If there are no buses on the resulting list, proceed to Step 7.

Step 3. Determine the 11 BES buses on the list with the highest maximum available calculated three phase short circuit MVA level. If the list has 11 or fewer buses, proceed to Step 7.

Step 4. Calculate the median MVA level of the 11 BES buses determined in Step 3.

Step 5. Multiply the median MVA level determined in Step 4 by 20 percent.

Step 6. Reduce the BES buses on the list to only those that have a maximum available calculated three phase short circuit MVA higher than the greater of:

- 1,500 MVA or
- 20 percent of median MVA level determined in Step 5.

Step 7. <u>If there are no BES buses on the list:</u> the procedure is complete and no FR and SER data will be required. Proceed to Step 9.

<u>If the list has 1 or more but less than or equal to 11 BES buses:</u> FR and SER data is required at the BES bus with the highest maximum available calculated three phase short circuit MVA as determined in Step 3. Proceed to Step 9.

If the list has more than 11 BES buses: SER and FR data is required on at least the 10 percent of the BES buses determined in Step 6 with the highest maximum available calculated three phase short circuit MVA. Proceed to Step 8.

Step 8. SER and FR data is required at additional BES buses on the list determined in Step 6. The aggregate of the number of BES buses determined in Step 7 and this Step will be at least 20 percent of the BES buses determined in Step 6.

The additional BES buses are selected, at the Transmission Owner's discretion, to provide maximum wide-area coverage for SER and FR data. The following BES bus locations are recommended:

- Electrically distant buses or electrically distant from other DME devices.
- Voltage sensitive areas.
- Cohesive load and generation zones.
- BES buses with a relatively high number of incident Transmission circuits.
- BES buses with reactive power devices.
- Major Facilities interconnecting outside the Transmission Owner's area.

Step 9. The list of monitored BES buses for SER and FR data for Requirement R1 is the aggregate of the BES buses determined in Steps 7 and 8.

Attachment 2

Sequence of Events Recording (SER) Data Format

(Requirement R11, Part 11.3)

Date, Time, Local Time Code, Substation, Device, State[1]

08/27/13, 23:58:57.110, -5, Sub 1, Breaker 1, Close

08/27/13, 23:58:57.082, -5, Sub 2, Breaker 2, Close

08/27/13, 23:58:47.217, -5, Sub 1, Breaker 1, Open

08/27/13, 23:58:47.214, -5, Sub 2, Breaker 2, Open

High Level Requirement Overview

[1] "OPEN" and "CLOSE" are used as examples. Other terminology such as TRIP, TRIP TO LOCKOUT, RECLOSE, etc. is also acceptable.

Requirement	Entity	Identify BES Buses	Notification	SER	FR	5 Year Re-evaluation
R1	TO	X	X	X	X	X
R2	TO | GO			X		
R3	TO | GO				X	
R4	TO | GO				X	

Requirement	Entity	Identify BES Elements	Notification	DDR	5 Year Re-evaluation
R5	RC	X	X	X	X
R6	TO			X	
R7	GO			X	
R8	TO | GO			X	
R9	TO | GO			X	

Requirement	Entity	Time Synchronization	Provide SER, FR, DDR Data	SER, FR, DDR Availability
R10	TO | GO	X		
R11	TO | GO		X	
R12	TO | GO			X

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 Functional Entities:

Because the Reliability Coordinator has the best wide-area view of the BES, the Reliability Coordinator is most suited to be responsible for determining the BES Elements for which dynamic Disturbance recording (DDR) data is required. The Transmission Owners and Generator Owners will have the responsibility for ensuring that adequate data is available for those BES Elements selected.

BES buses where sequence of events recording (SER) and fault recording (FR) data is required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their Systems to determine those buses. The Transmission Owners and Generator Owners that own BES Elements on those BES buses will have the responsibility for ensuring that adequate data is available.

Rationale for R1:

Analysis and reconstruction of BES events requires SER and FR data from key BES buses. Attachment 1 provides a uniform methodology to identify those BES buses. Repeated testing of the Attachment 1 methodology has demonstrated the proper distribution of SER and FR data collection. Review of actual BES short circuit data received from the industry in response to the DMSDT's data request (June 5, 2013 through July 5, 2013) illuminated a strong correlation between the available short circuit MVA at a Transmission bus and its relative size and importance to the BES based on (i) its voltage level, (ii) the number of Transmission Lines and other BES Elements connected to the BES bus, and (iii) the number and size of generating units connected to the bus. BES buses with a large short circuit MVA level are BES Elements that have a significant effect on System reliability and performance. Conversely, BES buses with very low short circuit MVA levels seldom cause wide-area or cascading System events, so SER and FR data from those BES Elements are not as significant. After analyzing and reviewing the collected data submittals from across the continent, the threshold MVA values were chosen to provide sufficient data for event analysis using engineering and operational judgment.

Concerns have existed that the defined methodology for bus selection will overly concentrate data to selected BES buses. For the purpose of PRC-002-2, there are a minimum number of BES buses for which SER and FR data is required based on the short circuit level. With these concepts and the objective being sufficient recording coverage for event analysis, the DMSDT developed the procedure in Attachment 1 that utilizes the maximum available calculated three phase short circuit MVA. This methodology ensures comparable and sufficient coverage for SER and FR data regardless of variations in the size and System topology of Transmission Owners across all Interconnections. Additionally, this methodology provides a degree of flexibility for the use of judgment in the selection process to ensure sufficient distribution.

BES buses where SER and FR data is required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their Systems to determine those buses.

Each Transmission Owner must re-evaluate the list of BES buses at least every five calendar years to address System changes since the previous evaluation. Changes to the BES do not mandate immediate inclusion of BES buses into the currently enforced list, but the list of BES buses will be re-evaluated at least every five calendar years to address System changes since the previous evaluation.

Since there may be multiple owners of equipment that comprise a BES bus, the notification required in R1 is necessary to ensure all owners are notified.

A 90-calendar day notification deadline provides adequate time for the Transmission Owner to make the appropriate determination and notification.

Rationale for R2:
The intent is to capture SER data for the status (open/close) of the circuit breakers that can interrupt the current flow through each BES Element connected to a BES bus. Change of state of circuit breaker position, time stamped according to Requirement R10 to a time synchronized clock, provides the basis for assembling the detailed sequence of events timeline of a power System Disturbance. Other status monitoring nomenclature can be used for devices other than circuit breakers.

Rationale for R3:
The required electrical quantities may either be directly measured or determinable if sufficient FR data is captured (e.g. residual or neutral current if the phase currents are directly measured). In order to cover all possible fault types, all BES bus phase-to-neutral voltages are required to be determinable for each BES bus identified in Requirement R1. BES bus voltage data is adequate for System Disturbance analysis. Phase current and residual current are required to distinguish between phase faults and ground faults. It also facilitates determination of the fault location and cause of relay operation. For transformers (Part 3.2.1), the data may be from either the high-side or the low-side of the transformer. Generator step-up transformers (GSUs) and leads that connect the GSU transformer(s) to the Transmission System that are used exclusively to export energy directly from a BES generating unit or generating plant are excluded from Requirement R3 because the fault current contribution from a generator to a fault on the Transmission System will be captured by FR data on the Transmission System, and Transmission System FR will capture faults on the generator interconnection.

Generator Owners may install this capability or, where the Transmission Owners already have suitable FR data, contract with the Transmission Owner. However, when required, the Generator Owner is still responsible for the provision of this data.

Rationale for R4:
Time stamped pre- and post-trigger fault data aid in the analysis of power System operations and determination if operations were as intended. System faults generally persist for a short time period, thus a 30-cycle total minimum record length is adequate. Multiple records allow for legacy microprocessor relays which, when time-synchronized, are capable of providing adequate fault data but not capable of providing fault data in a single record with 30-contiguous cycles total.

A minimum recording rate of 16 samples per cycle (960 Hz) is required to get sufficient point on wave data for recreating accurate fault conditions.

Rationale for R5:
DDR is used for capturing the BES transient and post-transient response following Disturbances, and the data is used for event analysis and validating System performance. DDR plays a critical role in wide-area Disturbance analysis, and Requirement R5 ensures there is adequate wide-area coverage of DDR data for specific BES Elements to facilitate accurate and efficient event analysis. The Reliability Coordinator has the best wide-area view of the System and needs to ensure that there are sufficient BES Elements identified for DDR data capture. The identification of BES Elements requiring DDR data as per Requirement R5 is based upon industry experience with wide-area Disturbance analysis and the need for adequate data to facilitate event analysis. Ensuring data is captured for these BES Elements will significantly improve the accuracy of analysis and understanding of why an event occurred, not simply what occurred.

From its experience with changes to the Bulk Electric System that would affect DDR, the DMSDT decided that the five calendar year re-evaluation of the list is a reasonable interval for this review. Changes to the BES do not mandate immediate inclusion of BES Elements into the in force list, but the list of BES Elements will be re-evaluated at least every five calendar years to address System changes since the previous evaluation. However, this standard does not preclude the Reliability Coordinator from performing this re-evaluation more frequently to capture updated BES Elements.

The Reliability Coordinator must notify all owners of the selected BES Elements that DDR data is required for this standard. The Reliability Coordinator is only required to share the list of selected BES Elements that each Transmission Owner and Generator Owner respectively owns, not the entire list. This communication of selected BES Elements is required to ensure that the owners of the respective BES Elements are aware of their responsibilities under this standard.

Implementation of the monitoring equipment is the responsibility of the respective Transmission Owners and Generator Owners, the timeline for installing this capability is outlined in the Implementation Plan, and starts from notification of the list from the Reliability Coordinator. Data for each BES Element as defined by the Reliability Coordinator must be provided; however, this data can be either directly measured or accurately calculated. With the exception of HVDC circuits, DDR data is only required for one end or terminal of the BES Elements selected. For example, DDR data must be provided for at least one terminal of a

Transmission Line or generator step-up (GSU) transformer, but not both terminals. For an interconnection between two Reliability Coordinators, each Reliability Coordinator will consider this interconnection independently, and are expected to work cooperatively to determine how to monitor the BES Elements that require DDR data. For an interconnection between two TO's, or a TO and a GO, the Reliability Coordinator will determine which entity will provide the data. The Reliability Coordinator will notify the owners that their BES Elements require DDR data.

Refer to the Guidelines and Technical Basis Section for more detail on the rationale and technical reasoning for each identified BES Element in Requirement R5, Part 5.1; monitoring these BES Elements with DDR will facilitate thorough and informative event analysis of wide-area Disturbances on the BES. Part 5.2 is included to ensure wide-area coverage across all Reliability Coordinators. It is intended that each Reliability Coordinator will have DDR data for one BES Element and at least one additional BES Element per 3,000 MW of its historical simultaneous peak System Demand.

Rationale for R6:
DDR is used to measure transient response to System Disturbances during a relatively balanced post-fault condition. Therefore, it is sufficient to provide a phase-to-neutral voltage or positive sequence voltage. The electrical quantities can be determined (calculated, derived, etc.).

Because all of the BES buses within a location are at the same frequency, one frequency measurement is adequate.

The data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a BES bus are closed.

Rationale for R7:
A crucial part of wide-area Disturbance analysis is understanding the dynamic response of generating resources. Therefore, it is necessary for Generator Owners to have DDR at either the high- or low-side of the generator step-up transformer (GSU) measuring the specified electrical quantities to adequately capture generator response. This standard defines the 'what' of DDR, not the 'how'. Generator Owners may install this capability or, where the Transmission Owners already have suitable DDR data, contract with the Transmission Owner. However, the Generator Owner is still responsible for the provision of this data.

Rationale for R8:
Large scale System outages generally are an evolving sequence of events that occur over an extended period of time, making DDR data essential for event analysis. Data available pre- and post-contingency helps identify the causes and effects of each event leading to outages. Therefore, continuous recording and storage are necessary to ensure sufficient data is available for the entire event.
Existing DDR data recording across the BES may not record continuously. To accommodate its use for the purposes of this standard, triggered records are acceptable if the equipment was installed prior to the effective date of this standard. The frequency triggers are defined based on the dynamic response associated with each Interconnection. The undervoltage trigger is

defined to capture possible delayed undervoltage conditions such as Fault Induced Delayed Voltage Recovery (FIDVR).

Rationale for R9:
An input sampling rate of at least 960 samples per second, which corresponds to 16 samples per cycle on the input side of the DDR equipment, ensures adequate accuracy for calculation of recorded measurements such as complex voltage and frequency.
An output recording rate of electrical quantities of at least 30 times per second refers to the recording and measurement calculation rate of the device. Recorded measurements of at least 30 times per second provide adequate recording speed to monitor the low frequency oscillations typically of interest during power System Disturbances.

Rationale for R10:
Time synchronization of Disturbance monitoring data is essential for time alignment of large volumes of geographically dispersed records from diverse recording sources. Coordinated Universal Time (UTC) is a recognized time standard that utilizes atomic clocks for generating precision time measurements. All data must be provided in UTC formatted time either with or without the local time offset, expressed as a negative number (the difference between UTC and the local time zone where the measurements are recorded).
Accuracy of time synchronization applies only to the clock used for synchronizing the monitoring equipment. The equipment used to measure the electrical quantities must be time synchronized to ± 2 ms accuracy; however, accuracy of the application of this time stamp and therefore the accuracy of the data itself is not mandated. This is because of inherent delays associated with measuring the electrical quantities and events such as breaker closing, measurement transport delays, algorithm and measurement calculation techniques, etc. Ensuring that the monitoring devices internal clocks are within ± 2 ms accuracy will suffice with respect to providing time synchronized data.

Rationale for R11:
Wide-area Disturbance analysis includes data recording from many devices and entities. Standardized formatting and naming conventions of these files significantly improves timely analysis.

Providing the data within 30-calendar days (or the granted extension time), subject to Part 11.1, allows for reasonable time to collect the data and perform any necessary computations or formatting.

Data is required to be retrievable for 10-calendar days inclusive of the day the data was recorded, i.e. a 10-calendar day rolling window of available data. Data hold requests are usually initiated the same or next day following a major event for which data is requested. A 10-calendar day time frame provides a practical limit on the duration of data required to be stored and informs the requesting entities as to how long the data will be available. The requestor of data has to be aware of the Part 11.1 10-calendar day retrievability because requiring data retention for a longer period of time is expensive and unnecessary.

SER data shall be provided in a simple ASCII .CSV format as outlined in Attachment 2. Either equipment can provide the data or a simple conversion program can be used to convert files into this format. This will significantly improve the data format for event records, enabling the use of software tools for analyzing the SER data.

Part 11.4 specifies FR and DDR data files be provided in conformance with IEEE C37.111, IEEE Standard for Common Format for Transient Exchange (COMTRADE), revision 1999 or later. The use of IEEE C37.111-1999 or later is well established in the industry. C37.111-2013 is a version of COMTRADE that includes an annex describing the application of the COMTRADE standard to synchrophasor data; however, version C37.111-1999 is commonly used in the industry today.

Part 11.5 uses a standardized naming format, C37.232-2011, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME), for providing Disturbance monitoring data. This file format allows a streamlined analysis of large Disturbances, and includes critical records such as local time offset associated with the synchronization of the data.

Rationale for R12:
Each Transmission Owner and Generator Owner who owns equipment used for collecting the data required for this standard must repair any failures within 90-calendar days to ensure that adequate data is available for event analysis. If the Disturbance monitoring capability cannot be restored within 90-calendar days (e.g. budget cycle, service crews, vendors, needed outages, etc.), the entity must develop a Corrective Action Plan (CAP) for restoring the data recording capability. The timeline required for the CAP depends on the entity and the type of data required. It is treated as a failure if the recording capability is out of service for maintenance and/or testing for greater than 90-calendar days. An outage of the monitored BES Element does not constitute a failure of the Disturbance monitoring capability.

Guidelines and Technical Basis Section

Introduction

The emphasis of PRC-002-2 is not on how Disturbance monitoring data is captured, but what Bulk Electric System data is captured. There are a variety of ways to capture the data PRC-002-2 addresses, and existing and currently available equipment can meet the requirements of this standard. PRC-002-2 also addresses the importance of addressing the availability of Disturbance monitoring capability to ensure the completeness of BES data capture.

The data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a bus are closed.

PRC-002-2 addresses “what” data is recorded, not “how” it is recorded.

Guideline for Requirement R1:

Sequence of events and fault recording for the analysis, reconstruction, and reporting of System Disturbances is important. However, SER and FR data is not required at every BES bus on the BES to conduct adequate or thorough analysis of a Disturbance. As major tools of event analysis, the time synchronized time stamp for a breaker change of state and the recorded waveforms of voltage and current for individual circuits allows the precise reconstruction of events of both localized and wide-area Disturbances.

More quality information is always better than less when performing event analysis. However, 100 percent coverage of all BES Elements is not practical nor required for effective analysis of wide-area Disturbances. Therefore, selectivity of required BES buses to monitor is important for the following reasons:

1. Identify key BES buses with breakers where crucial information is available when required.
2. Avoid excessive overlap of coverage.
3. Avoid gaps in critical coverage.
4. Provide coverage of BES Elements that could propagate a Disturbance.
5. Avoid mandates to cover BES Elements that are more likely to be a casualty of a Disturbance rather than a cause.
6. Establish selection criteria to provide effective coverage in different regions of the continent.

The major characteristics available to determine the selection process are:

1. System voltage level;
2. The number of Transmission Lines into a substation or switchyard;
3. The number and size of connected generating units;
4. The available short circuit levels.

Although it is straightforward to establish criteria for the application of identified BES buses, analysis was required to establish a sound technical basis to fulfill the required objectives.

To answer these questions and establish criteria for BES buses of SER and FR, the DMSDT established a sub-team referred to as the Monitored Value Analysis Team (MVA Team). The MVA Team collected information from a wide variety of Transmission Systems throughout the continent to analyze Transmission buses by the characteristics previously identified for the selection process.

The MVA Team learned that the development of criteria is not possible for adequate SER and FR coverage, based solely upon simple, bright line characteristics, such as the number of lines into a substation or switchyard at a particular voltage level or at a set level of short circuit current. To provide the appropriate coverage, a relatively simple but effective Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data was developed. This Procedure, included as Attachment 1, assists entities in fulfilling Requirement R1 of the standard.

The Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data is weighted to buses with higher short circuit levels. This is chosen for the following reasons:

1. The method is voltage level independent.
2. It is likely to select buses near large generation centers.
3. It is likely to select buses where delayed clearing can cause Cascading.
4. Selected buses directly correlate to the Universal Power Transfer equation: Lower Impedance – increased power flows – greater System impact.

To perform the calculations of Attachment 1, the following information below is required and the following steps (provided in summary form) are required for Systems with more than 11 BES buses with three phase short circuit levels above 1,500 MVA.

1. Total number of BES buses in the Transmission System under evaluation.
   a. Only tangible substation or switchyard buses are included.
   b. Pseudo buses created for analysis purposes in System models are excluded.
2. Determine the three phase short circuit MVA for each BES bus.
3. Exclude BES buses from the list with short circuit levels below 1,500 MVA.
4. Determine the median short circuit for the top 11 BES buses on the list (position number 6).
5. Multiply median short circuit level by 20 percent.
6. Reduce the list of BES buses to those with short circuit levels higher than 20 percent of the median.
7. Apply SER and FR at BES buses with short circuit levels in the top 10 percent of the list (from 6).

8. Apply SER and FR at BES buses at an additional 10 percent of the list using engineering judgment, and allowing flexibility to factor in the following considerations:
   - Electrically distant BES buses or electrically distant from other DME devices
   - Voltage sensitive areas
   - Cohesive load and generation zones
   - BES buses with a relatively high number of incident Transmission circuits
   - BES buses with reactive power devices
   - Major facilities interconnecting outside the Transmission Owner's area.

For event analysis purposes, more valuable information is attained about generators and their response to System events pre- and post-contingency through DDR data versus SER or FR records. SER data of the opening of the primary generator output interrupting devices (e.g. synchronizing breaker) may not reliably indicate the actual time that a generator tripped; for instance, when it trips on reverse power after loss of its prime mover (e.g. combustion or steam turbine). As a result, this standard only requires DDR data.

The re-evaluation interval of five years was chosen based on the experience of the DMSDT to address changing System configurations while creating balance in the frequency of re-evaluations.

Guideline for Requirement R2:

Analyses of wide-area Disturbances often begin by evaluation of SERs to help determine the initiating event(s) and follow the Disturbance propagation. Recording of breaker operations help determine the interruption of line flows while generator loading is best determined by DDR data, since generator loading can be essentially zero regardless of breaker position. However, generator breakers directly connected to an identified BES bus are required to have SER data captured. It is important in event analysis to know when a BES bus is cleared regardless of a generator's loading.

Generator Owners are included in this requirement because a Generator Owner may, in some instances, own breakers directly connected to the Transmission Owner's BES bus.

Guideline for Requirement R3:

The BES buses for which FR data is required are determined based on the methodology described in Attachment 1 of the standard. The BES Elements connected to those BES buses for which FR data is required include:

- Transformers with a low-side operating voltage of 100kV or above
- Transmission Lines

Only those BES Elements that are identified as BES as defined in the latest in effect NERC definition are to be monitored. For example, radial lines or transformers with low-side voltage less than 100kV are not included.

FR data must be determinable from each terminal of a BES Element connected to applicable BES buses.

Generator step-up transformers (GSU) are excluded from the above based on the following:

- Current contribution from a generator in case of fault on the Transmission System will be captured by FR data on the Transmission System.
- For faults on the interconnection to generating facilities it is sufficient to have fault current data from the Transmission station end of the interconnection. Current contribution from a generator can be readily calculated if needed.

The DMSDT, after consulting with NERC's Event Analysis group, determined that DDR data from selected generator locations was more important for event analysis than FR data.

Recording of Electrical Quantities

For effective fault analysis it is necessary to know values of all phase and neutral currents and all phase-to-neutral voltages. Based on such FR data it is possible to determine all fault types. FR data also augments SERs in evaluating circuit breaker operation.

Current Recordings

The required electrical quantities are normally directly measured. Certain quantities can be derived if sufficient data is measured, for example residual or neutral currents.
Since a Transmission System is generally well balanced, with phase currents having essentially similar magnitudes and phase angle differences of 120°, during normal conditions there is negligible neutral (residual) current. In case of a ground fault the resulting phase current imbalance produces residual current that can be either measured or calculated.

Neutral current, also known as ground or residual current $\mathbf{I}_r$, is calculated as a sum of vectors of three phase currents:

$\mathbf{I}_r = 3 \bullet \mathbf{I}_0 = \mathbf{I}_A + \mathbf{I}_B + \mathbf{I}_C$

$\mathbf{I}_0$ - Zero-sequence current

$\mathbf{I}_A$, $\mathbf{I}_B$, $\mathbf{I}_C$ - Phase current (vectors)

Another example of how required electrical quantities can be derived is based on Kirchhoff's Law. Fault currents for one of the BES Elements connected to a particular BES bus can be derived as a vectorial sum of fault currents recorded at the other BES Elements connected to that BES bus.

Voltage Recordings

Voltages are to be recorded or accurately determined at applicable BES buses.

Guideline for Requirement R4:

Pre- and post-trigger fault data along with the SER breaker data, all time stamped to a common clock at millisecond accuracy, aid in the analysis of protection System operations after a fault to determine if a protection System operated as designed. Generally speaking, BES faults persist for a very short time period, approximately 1 to 30 cycles, thus a 30-cycle record length provides adequate data. Multiple records allow for legacy microprocessor relays which, when time synchronized to a common clock, are capable of providing adequate fault data but not capable of providing fault data in a single record with 30-contiguous cycles total.

A minimum recording rate of 16 samples per cycle is required to get accurate waveforms and to get 1 millisecond resolution for any digital input which may be used for FR.

FR triggers can be set so that when the monitored value on the recording device goes above or below the trigger value, data is recorded. Requirement R4, sub-Part 4.3.1 specifies a neutral (residual) overcurrent trigger for ground faults. Requirement R4, sub-Part 4.3.2 specifies a phase undervoltage or overcurrent trigger for phase-to-phase faults.

Guideline for Requirement R5:

DDR data is used for wide-area Disturbance monitoring to determine the System's electromechanical transient and post-transient response and validate System model performance. DDR is typically located based on strategic studies which include angular, frequency, voltage, and oscillation stability. However, for adequately monitoring the System's dynamic response and ensuring sufficient coverage to determine System performance, DDR is required for key BES Elements in addition to a minimum requirement of DDR coverage.

Each Reliability Coordinator is required to identify sufficient DDR data capture for, at a minimum, one BES Element and then one additional BES Element per 3,000 MW of historical simultaneous peak System Demand. This DDR data is included to provide adequate System wide coverage across an Interconnection. To clarify, if any of the key BES Elements requiring DDR monitoring are within the Reliability Coordinator Area, DDR data capability is required. If a Reliability Coordinator does not meet the requirements of Part 5.1, additional coverage had to be specified.

Loss of large generating resources poses a frequency and angular stability risk for all Interconnections across North America. Data capturing the dynamic response of these machines during a Disturbance helps the analysis of large Disturbances. Having data regarding generator dynamic response to Disturbances greatly improves understanding of ***why*** an event occurs rather than what occurred. To determine and provide the basis for unit size criteria, the DMSDT acquired specific generating unit data from NERC's Generating Availability Data System (GADS) program. The data contained generating unit size information for each generating unit in North America which was reported in 2013 to the NERC GADS program. The DMSDT analyzed the spreadsheet data to determine: (i) how many units were above or below selected size

thresholds; and (ii) the aggregate sum of the ratings of the units within the boundaries of those thresholds. Statistical information about this data was then produced, i.e. averages, means and percentages. The DMSDT determined the following basic information about the generating units of interest (current North America fleet, i.e. units reporting in 2013) included in the spreadsheet:

- The number of individual generating units in total included in the spreadsheet.
- The number of individual generating units rated at 20 MW or larger included in the spreadsheet. These units would generally require that their owners be registered as GOs in the NERC CMEP.
- The total number of units within selected size boundaries.
- The aggregate sum of ratings, in MWs, of the units within the boundaries of those thresholds.

The information in the spreadsheet does not provide information by which the plant information location of each unit can be determined, i.e. the DMSDT could not use the information to determine which units were located together at a given generation site or facility.

From this information, the DMSDT was able to reasonably speculate the generating unit size thresholds proposed in Requirement R5, sub-Part 5.1.1 of the standard. Generating resources intended for DDR data recording are those individual units with gross nameplate ratings "greater than or equal to 500 MVA". The 500 MVA individual unit size threshold was selected because this number roughly accounts for 47 percent of the generating capacity in NERC footprint while only requiring DDR coverage on about 12.5 percent of the generating units. As mentioned, there was no data pertaining to unit location for aggregating plant/facility sizes. However, Requirement R5, sub-Part 5.1.1 is included to capture larger units located at large generating plants which could pose a stability risk to the System if multiple large units were lost due to electrical or non-electrical contingencies. For generating plants, each individual generator at the plant/facility with a gross nameplate rating greater than or equal to 300 MVA must have DDR where the gross nameplate rating of the plant/facility is greater than or equal to 1,000 MVA. The 300 MVA threshold was chosen based on the DMSDT's judgment and experience. The incremental impact to the number of units requiring monitoring is expected to be relatively low. For combined cycle plants where only one generator has a rating greater than or equal to 300MVA, that is the only generator that would need DDR.

Permanent System Operating Limits (SOLs) are used to operate the System within reliable and secure limits. In particular, SOLs related to angular or voltage stability have a significant impact on BES reliability and performance. Therefore, at least one BES Element of an SOL should be monitored.

The draft standard requires "One or more BES Elements that are part of an Interconnection Reliability Operating Limits (IROLs)." Interconnection Reliability Operating Limits (IROLs) are included because the risk of violating these limits poses a risk to System stability and the potential for cascading outages. IROLs may be defined by a single or multiple monitored BES

Element(s) and contingent BES Element(s). The standard does not dictate selection of the contingent and/or monitored BES Elements. Rather the Drafting Team believes this determination is best made by the Reliability Coordinator for each IROL considered based on the severity of violating this IROL.

Locations where an undervoltage load shedding (UVLS) program is deployed are prone to voltage instability since they are generally areas of significant Demand. The Reliability Coordinator will identify these areas where a UVLS is in service and identify a useful and effective BES Element to monitor for DDR such that action of the UVLS or voltage instability on the BES could be captured. For example, a major 500kV or 230kV substation on the EHV System close to the load pocket where the UVLS is deployed would likely be a valuable electrical location for DDR coverage and would aid in post-Disturbance analysis of the load area's response to large System excursions (voltage, frequency, etc.).

Guideline for Requirement R6:

DDR data shows transient response to System Disturbances after a fault is cleared (post-fault), under a relatively balanced operating condition. Therefore, it is sufficient to provide a single phase-to-neutral voltage or positive sequence voltage. Recording of all three phases of a circuit is not required, although this may be used to compute and record the positive sequence voltage.

The bus where a voltage measurement is required is based on the list of BES Elements defined by the Reliability Coordinator in Requirement R5. The intent of the standard is not to require a separate voltage measurement of each BES Element where a common bus voltage measurement is available. For example, a breaker-and-a-half or double-bus configuration with a North (or East) Bus and South (or West) Bus, would require both buses to have voltage recording because either can be taken out of service indefinitely with the targeted BES Element remaining in service. This may be accomplished either by recording both bus voltages separately, or by providing a selector switch to connect either of the bus voltage sources to a single recording input of the DDR device. This component of the requirement is therefore included to mitigate the potential of failed frequency, phase angle, real power, and reactive power calculations due to voltage measurements removed from service while sufficient voltage measurement is actually available during these operating conditions.

It must be emphasized that the data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a bus are closed.

When current recording is required, it should be on the same phase as the voltage recording taken at the location if a single phase-to-neutral voltage is provided. Positive sequence current recording is also acceptable.

For all circuits where current recording is required, Real and Reactive Power will be recorded on a three phase basis. These recordings may be derived either from phase quantities or from positive sequence quantities.

Guideline for Requirement R7:

All Guidelines specified for Requirement R6 apply to Requirement R7. Since either the high- or low-side windings of the generator step-up transformer (GSU) may be connected in delta, phase-to-phase voltage recording is an acceptable voltage recording. As was explained in the Guideline for Requirement R6, the BES is operating under a relatively balanced operating condition and, if needed, phase-to-neutral quantities can be derived from phase-to-phase quantities.

Again it must be emphasized that the data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a bus are closed.

Guideline for Requirement R8:

Wide-area System outages are generally an evolving sequence of events that occur over an extended period of time, making DDR data essential for event analysis. Pre- and post-contingency data helps identify the causes and effects of each event leading to the outages. This drives a need for continuous recording and storage to ensure sufficient data is available for the entire Disturbance.

Transmission Owners and Generator Owners are required to have continuous DDR for the BES Elements identified in Requirement R6. However, this requirement recognizes that legacy equipment may exist for some BES Elements that do not have continuous data recording capabilities. For equipment that was installed prior to the effective date of the standard, triggered DDR records of three minutes are acceptable using at least one of the trigger types specified in Requirement R8, Part 8.2:

- Off nominal frequency triggers are used to capture high- or low-frequency excursions of significant size based on the Interconnection size and inertia.
- Rate of change of frequency triggers are used to capture major changes in System frequency which could be caused by large changes in generation or load, or possibly changes in System impedance.
- The undervoltage trigger specified in this standard is provided to capture possible sustained undervoltage conditions such as Fault Induced Delayed Voltage Recovery (FIDVR) events. A sustained voltage of 85 percent is outside normal schedule operating voltages and is sufficiently low to capture abnormal voltage conditions on the BES.

Guideline for Requirement R9:

DDR data contains the dynamic response of a power System to a Disturbance and is used for analyzing complex power System events. This recording is typically used to capture short-term

and long-term Disturbances, such as a power swing. Since the data of interest is changing over time, DDR data is normally stored in the form of RMS values or phasor values, as opposed to directly sampled data as found in FR data.

The issue of the sampling rate used in a recording instrument is quite important for at least two reasons: the anti-aliasing filter selection and accuracy of signal representation. The anti-aliasing filter selection is associated with the requirement of a sampling rate at least twice the highest frequency of a sampled signal. At the same time, the accuracy of signal representation is also dependent on the selection of the sampling rate. In general, the higher the sampling rate, the better the representation. In the abnormal conditions of interest (e.g. faults or other Disturbances); the input signal may contain frequencies in the range of 0-400 Hz. Hence, the rate of 960 samples per second (16 samples/cycle) is considered an adequate sampling rate that satisfies the input signal requirements.

In general, dynamic events of interest are: inter-area oscillations, local generator oscillations, wind turbine generator torsional modes, HVDC control modes, exciter control modes, and steam turbine torsional modes. Their frequencies range from 0.1-20 Hz. In order to reconstruct these dynamic events, a minimum recording time of 30 times per second is required.

Guideline for Requirement R10: Time synchronization of Disturbance monitoring data allows for the time alignment of large volumes of geographically dispersed data records from diverse recording sources. A universally recognized time standard is necessary to provide the foundation for this alignment. Coordinated Universal Time (UTC) is the foundation used for the time alignment of records. It is an international time standard utilizing atomic clocks for generating precision time measurements at fractions of a second levels. The local time offset, expressed as a negative number, is the difference between UTC and the local time zone where the measurements are recorded.

Accuracy of time synchronization applies only to the clock used for synchronizing the monitoring equipment.

Time synchronization accuracy is specified in response to Recommendation 12b in the NERC August, 2003, Blackout Final NERC Report Section V Conclusions and Recommendations:

“Recommendation 12b: Facilities owners shall, in accordance with regional criteria, upgrade existing dynamic recorders to include GPS time synchronization…”

Also, from the U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout, November 2003, in the United States and Canada, page 103:

“Establishing a precise and accurate sequence of outage-related events was a critical building block for the other parts of the investigation. One of the key problems in developing this sequence was that although much of the data pertinent to an event was time-stamped, there was some variance from source to source in how the time-stamping was done, and not all of the time-stamps were synchronized…”

From NPCC's SP6 Report Synchronized Event Data Reporting, revised March 31, 2005, the investigation by the authoring working group revealed that existing GPS receivers can be expected to provide a time code output which has an uncertainty on the order of 1 millisecond, uncertainty being a quantitative descriptor.

Guideline for Requirement R11:

This requirement directs the applicable entities, upon requests from the Reliability Coordinator, Regional Entity or NERC, to provide SER and FR data for BES buses determined in Requirement R1 and DDR data for BES Elements determined as per Requirement R5. To facilitate the analysis of BES Disturbances, it is important that the data is provided to the requestor within a reasonable period of time.

Requirement R11, Part 11.1 specifies the maximum time frame of 30-calendar days to provide the data. Thirty calendar days is a reasonable time frame to allow for the collection of data, and submission to the requestor. An entity may request an extension of the 30-day submission requirement. If granted by the requestor, the entity must submit the data within the approved extended time.

Requirement R11, Part 11.2 specifies that the minimum time period of 10-calendar days inclusive of the day the data was recorded for which the data will be retrievable. With the equipment in use that has the capability of recording data, having the data retrievable for the 10-calendar days is realistic and doable. It is important to note that applicable entities should account for any expected delays in retrieving data and this may require devices to have data available for more than 10 days. To clarify the 10-calendar day time frame, an incident occurs on Day 1. If a request for data is made on Day 6, then that data has to be provided to the requestor within 30-calendar days after a request or a granted time extension. However, if a request for the data is made on Day 11, that is outside the 10-calendar days specified in the requirement, and an entity would not be out of compliance if it did not have the data.

Requirement R11, Part 11.3 specifies a Comma Separated Value (CSV) format according to Attachment 2 for the SER data. It is necessary to establish a standard format as it will be incorporated with other submitted data to provide a detailed sequence of events timeline of a power System Disturbance.

Requirement R11, Part 11.4 specifies the IEEE C37.111 COMTRADE format for the FR and DDR data. The IEEE C37.111 is the Standard for Common Format for Transient Data Exchange and is well established in the industry. It is necessary to specify a standard format as multiple submissions of data from many sources will be incorporated to provide a detailed analysis of a power System Disturbance. The latest revision of COMTRADE (C37.111-2013) includes an annex describing the application of the COMTRADE standard to synchophasor data.

Requirement R11, Part 11.5 specifies the IEEE C37.232 COMNAME format for naming the data files of the SER, FR and DDR. The IEEE C37.232 is the Standard for Common Format for Naming Time Sequence Data Files. The first version was approved in 2007. From the August 14, 2003 blackout there were thousands of Fault Recording data files collected. The collected data files

did not have a common naming convention and it was therefore difficult to discern which files came from which utilities and which ones were captured by which devices. The lack of a common naming practice seriously hindered the investigation process. Subsequently, and in its initial report on the blackout, NERC stressed the need for having a common naming practice and listed it as one of its top ten recommendations.

Guideline for Requirement R12:

This requirement directs the respective owners of Transmission and Generator equipment to be alert to the proper functioning of equipment used for SER, FR, and DDR data capabilities for the BES buses and BES Elements, which were established in Requirements R1 and R5. The owners are to restore the capability within 90-calendar days of discovery of a failure. This requirement is structured to recognize that the existence of a "reasonable" amount of capability out-of-service does not result in lack of sufficient data for coverage of the System. Furthermore, 90-calendar days is typically sufficient time for repair or maintenance to be performed. However, in recognition of the fact that there may be occasions for which it is not possible to restore the capability within 90-calendar days, the requirement further provides that, for such cases, the entity submit a Corrective Action Plan (CAP) to the Regional Entity and implement it. These actions are considered to be appropriate to provide for robust and adequate data availability.

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 Board of Trustees.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** Disturbance Monitoring and Reporting Requirements

2. **Number:** PRC-002-32

3. **Purpose:** To have adequate data available to facilitate analysis of Bulk Electric System (BES) Disturbances.

4. **Applicability:**

Functional Entities:

4.1 Reliability Coordinator~~The Responsible Entity is:~~

~~Eastern Interconnection – Planning Coordinator~~

~~**4.1.1 4.1.2 ERCOT Interconnection – Planning Coordinator or Reliability Coordinator**~~

~~**4.1.3** Western Interconnection – Reliability Coordinator~~

~~**4.1.4** Quebec Interconnection – Planning Coordinator or Reliability Coordinator~~

4.2 Transmission Owner

4.3 Generator Owner

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

B. Requirements and Measures

R1. Each Transmission Owner shall: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. Identify BES buses for which sequence of events recording (SER) and fault recording (FR) data is required by using the methodology in PRC-002-2, Attachment 1.

1.2. Notify other owners of BES Elements connected to those BES buses, if any, within 90-calendar days of completion of Part 1.1, that those BES Elements require SER data and/or FR data.

1.3. Re-evaluate all BES buses at least once every five calendar years in accordance with Part 1.1 and notify other owners, if any, in accordance with Part 1.2, and implement the re-evaluated list of BES buses as per the Implementation Plan.

M1. The Transmission Owner has a dated (electronic or hard copy) list of BES buses for which SER and FR data is required, identified in accordance with PRC-002-2, Attachment 1, and evidence that all BES buses have been re-evaluated within the required intervals under Requirement R1. The Transmission Owner will also have

dated (electronic or hard copy) evidence that it notified other owners in accordance with Requirement R1.

R2. Each Transmission Owner and Generator Owner shall have SER data for circuit breaker position (open/close) for each circuit breaker it owns connected directly to the BES buses identified in Requirement R1 and associated with the BES Elements at those BES buses. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of SER data for circuit breaker position as specified in Requirement R2. Evidence may include, but is not limited to: (1) documents describing the device interconnections and configurations which may include a single design standard as representative for common installations; or (2) actual data recordings; or (3) station drawings.

R3. Each Transmission Owner and Generator Owner shall have FR data to determine the following electrical quantities for each triggered FR for the BES Elements it owns connected to the BES buses identified in Requirement R1: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1 Phase-to-neutral voltage for each phase of each specified BES bus.

3.2 Each phase current and the residual or neutral current for the following BES Elements:

3.2.1 Transformers that have a low-side operating voltage of 100kV or above.

3.2.2 Transmission Lines.

M3. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of FR data that is sufficient to determine electrical quantities as specified in Requirement R3. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations which may include a single design standard as representative for common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R4. Each Transmission Owner and Generator Owner shall have FR data as specified in Requirement R3 that meets the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

4.1 A single record or multiple records that include:

- A pre-trigger record length of at least two cycles and a total record length of at least 30-cycles for the same trigger point, or
- At least two cycles of the pre-trigger data, the first three cycles of the post-trigger data, and the final cycle of the fault as seen by the fault recorder.

4.2 A minimum recording rate of 16 samples per cycle.

4.3 Trigger settings for at least the following:

4.3.1 Neutral (residual) overcurrent.

4.3.2 Phase undervoltage or overcurrent.

M4. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that FR data meets Requirement R4. Evidence may include, but is not limited to: (1) documents describing the device specification (R4, Part 4.2) and device configuration or settings (R4, Parts 4.1 and 4.3), or (2) actual data recordings or derivations.

R5. Each Reliability Coordinator~~Responsible Entity~~ shall: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

5.1 Identify BES Elements for which dynamic Disturbance recording (DDR) data is required, including the following:

5.1.1 Generating resource(s) with:

5.1.1.1 Gross individual nameplate rating greater than or equal to 500 MVA.

5.1.1.2 Gross individual nameplate rating greater than or equal to 300 MVA where the gross plant/facility aggregate nameplate rating is greater than or equal to 1,000 MVA.

5.1.2 Any one BES Element that is part of a stability (angular or voltage) related System Operating Limit (SOL).

5.1.3 Each terminal of a high voltage direct current (HVDC) circuit with a nameplate rating greater than or equal to 300 MVA, on the alternating current (AC) portion of the converter.

5.1.4 One or more BES Elements that are part of an Interconnection Reliability Operating Limit (IROL).

5.1.5 Any one BES Element within a major voltage sensitive area as defined by an area with an in-service undervoltage load shedding (UVLS) program.

5.2 Identify a minimum DDR coverage, inclusive of those BES Elements identified in Part 5.1, of at least:

5.2.1 One BES Element; and

5.2.2 One BES Element per 3,000 MW of the Reliability Coordinator's~~Responsible Entity's~~ historical simultaneous peak System Demand.

5.3 Notify all owners of identified BES Elements, within 90-calendar days of completion of Part 5.1, that their respective BES Elements require DDR data when requested.

5.4 Re-evaluate all BES Elements at least once every five calendar years in accordance with Parts 5.1 and 5.2, and notify owners in accordance with Part 5.3 to implement the re-evaluated list of BES Elements as per the Implementation Plan.

M5. The Reliability Coordinator~~Responsible Entity~~ has a dated (electronic or hard copy) list of BES Elements for which DDR data is required, developed in accordance with Requirement R5, Part 5.1 and Part 5.2; and re-evaluated in accordance with Part 5.4. The Reliability Coordinator~~Responsible Entity~~ has dated evidence (electronic or hard copy) that each Transmission Owner or Generator Owner has been notified in accordance with Requirement 5, Part 5.3. Evidence may include, but is not limited to: letters, emails, electronic files, or hard copy records demonstrating transmittal of information.

R6. Each Transmission Owner shall have DDR data to determine the following electrical quantities for each BES Element it owns for which it received notification as identified in Requirement R5: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

6.1 One phase-to-neutral or positive sequence voltage.

6.2 The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R6, Part 6.1, or the positive sequence current.

6.3 Real Power and Reactive Power flows expressed on a three phase basis corresponding to all circuits where current measurements are required.

6.4 Frequency of any one of the voltage(s) in Requirement R6, Part 6.1.

M6. The Transmission Owner has evidence (electronic or hard copy) of DDR data to determine electrical quantities as specified in Requirement R6. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R7. Each Generator Owner shall have DDR data to determine the following electrical quantities for each BES Element it owns for which it received notification as identified in Requirement R5: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

7.1 One phase-to-neutral, phase-to-phase, or positive sequence voltage at either the generator step-up transformer (GSU) high-side or low-side voltage level.

7.2 The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R7, Part 7.1, phase current(s) for any phase-to-phase voltages, or positive sequence current.

7.3 Real Power and Reactive Power flows expressed on a three phase basis corresponding to all circuits where current measurements are required.

7.4 Frequency of at least one of the voltages in Requirement R7, Part 7.1.

M7. The Generator Owner has evidence (electronic or hard copy) of DDR data to determine electrical quantities as specified in Requirement R7. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for

common installations; or (2) actual data recordings or derivations; or (3) station drawings.

R8. Each Transmission Owner and Generator Owner responsible for DDR data for the BES Elements identified in Requirement R5 shall have continuous data recording and storage. If the equipment was installed prior to the effective date of this standard and is not capable of continuous recording, triggered records must meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

8.1 Triggered record lengths of at least three minutes.

8.2 At least one of the following three triggers:

- Off nominal frequency trigger set at:

	Low	High
○ Eastern Interconnection	<59.75 Hz	>61.0 Hz
○ Western Interconnection	<59.55 Hz	>61.0 Hz
○ ERCOT Interconnection	<59.35 Hz	>61.0 Hz
○ Hydro-Quebec Interconnection	<58.55 Hz	>61.5 Hz

- Rate of change of frequency trigger set at:

○ Eastern Interconnection	< -0.03125 Hz/sec	> 0.125 Hz/sec
○ Western Interconnection	< -0.05625 Hz/sec	> 0.125 Hz/sec
○ ERCOT Interconnection	< -0.08125 Hz/sec	> 0.125 Hz/sec
○ Hydro-Quebec Interconnection	< -0.18125 Hz/sec	> 0.1875 Hz/sec

- Undervoltage trigger set no lower than 85 percent of normal operating voltage for a duration of 5 seconds.

M8. Each Transmission Owner and Generator Owner has dated evidence (electronic or hard copy) of data recordings and storage in accordance with Requirement R8. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations, which may include a single design standard as representative for common installations; or (2) actual data recordings.

R9. Each Transmission Owner and Generator Owner responsible for DDR data for the BES Elements identified in Requirement R5 shall have DDR data that meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

9.1 Input sampling rate of at least 960 samples per second.

9.2 Output recording rate of electrical quantities of at least 30 times per second.

M9. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that DDR data meets Requirement R9. Evidence may include, but is not limited to: (1) documents describing the device specification, device configuration, or settings (R9, Part 9.1; R9, Part 9.2); or (2) actual data recordings (R9, Part 9.2).

R10. Each Transmission Owner and Generator Owner shall time synchronize all SER and FR data for the BES buses identified in Requirement R1 and DDR data for the BES Elements identified in Requirement R5 to meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

10.1 Synchronization to Coordinated Universal Time (UTC) with or without a local time offset.

10.2 Synchronized device clock accuracy within ± 2 milliseconds of UTC.

M10. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) of time synchronization described in Requirement R10. Evidence may include, but is not limited to: (1) documents describing the device specification, configuration, or setting; (2) time synchronization indication or status; or 3) station drawings.

R11. Each Transmission Owner and Generator Owner shall provide, upon request, all SER and FR data for the BES buses identified in Requirement R1 and DDR data for the BES Elements identified in Requirement R5 to the Reliability Coordinator~~Responsible Entity~~, Regional Entity, or NERC in accordance with the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

11.1 Data will be retrievable for the period of 10-calendar days, inclusive of the day the data was recorded.

11.2 Data subject to Part 11.1 will be provided within 30-calendar days of a request unless an extension is granted by the requestor.

11.3 SER data will be provided in ASCII Comma Separated Value (CSV) format following Attachment 2.

11.4 FR and DDR data will be provided in electronic files that are formatted in conformance with C37.111, (IEEE Standard for Common Format for Transient Data Exchange (COMTRADE), revision C37.111-1999 or later.

11.5 Data files will be named in conformance with C37.232, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME), revision C37.232-2011 or later.

M11. The Transmission Owner or Generator Owner has evidence (electronic or hard copy) that data was submitted upon request in accordance with Requirement R11. Evidence may include, but is not limited to: (1) dated transmittals to the requesting

entity with formatted records; (2) documents describing data storage capability, device specification, configuration or settings; or (3) actual data recordings.

R12. Each Transmission Owner and Generator Owner shall, within 90-calendar days of the discovery of a failure of the recording capability for the SER, FR or DDR data, either: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- Restore the recording capability, or
- Submit a Corrective Action Plan (CAP) to the Regional Entity and implement it.

M12. The Transmission Owner or Generator Owner has dated evidence (electronic or hard copy) that meets Requirement R12. Evidence may include, but is not limited to: (1) dated reports of discovery of a failure, (2) documentation noting the date the data recording was restored, (3) SCADA records, or (4) dated CAP transmittals to the Regional Entity and evidence that it implemented the CAP.

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 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 Transmission Owner, Generator Owner, ~~Planning Coordinator,~~ and Reliability Coordinator 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 Owner shall retain evidence of Requirement R1, Measure M1 for five calendar years.

The Transmission Owner shall retain evidence of Requirement R6, Measure M6 for three calendar years.

The Generator Owner shall retain evidence of Requirement R7, Measure M7 for three calendar years.

The Transmission Owner and Generator Owner shall retain evidence of requested data provided as per Requirements R2, R3, R4, R8, R9, R10, R11, and R12, Measures M2, M3, M4, M8, M9, M10, M11, and M12 for three calendar years.

The ~~Responsible Entity (Planning Coordinator or~~ Reliability Coordinator~~, as applicable)~~ shall retain evidence of Requirement R5, Measure M5 for five calendar years.

If a Transmission Owner, Generator Owner, or Reliability Coordinator ~~Responsible Entity~~ is found non-compliant, it shall keep information related to the non-compliance until mitigation is completed and approved or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Lower	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 80 percent but less than 100 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by 30-calendar days or less. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying the other	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 70 percent but less than or equal to 80 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by greater than 30-calendar days and less than or equal to 60-calendar days. OR The Transmission Owner as directed by Requirement R1, Part	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for more than 60 percent but less than or equal to 70 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by greater than 60-calendar days and less than or equal to 90-calendar days. OR The Transmission Owner as directed by Requirement R1, Part	The Transmission Owner identified the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 for less than or equal to 60 percent of the required BES buses that they own. OR The Transmission Owner evaluated the BES buses as directed by Requirement R1, Part 1.1 or Part 1.3 but was late by greater than 90-calendar days. OR The Transmission Owner as directed by Requirement R1, Part 1.2 was late in notifying one or more other owners by

			owners by 10-calendar days or less.	1.2 was late in notifying the other owners by greater than 10-calendar days but less than or equal to 20-calendar days.	1.2 was late in notifying the other owners by greater than 20-calendar days but less than or equal to 30-calendar days.	greater than 30-calendar days.
R2	Long-term Planning	Lower	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 80 percent but less than 100 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 70 percent but less than or equal to 80 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 had more than 60 percent but less than or equal to 70 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.	Each Transmission Owner or Generator Owner as directed by Requirement R2 for less than or equal to 60 percent of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the BES buses identified in Requirement R1.
R3	Long-term Planning	Lower	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 80 percent but less than 100 percent of the total set of required electrical	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 70 percent but less than or equal to 80 percent of the total set of required	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 60 percent but less than or equal to 70 percent of the total set of required	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers less than or equal to 60 percent of the total set of required electrical quantities,

			quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.	electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.	electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.	which is the product of the total number of monitored BES Elements and the number of specified electrical quantities for each BES Element.
R4	Long-term Planning	Lower	The Transmission Owner or Generator Owner had FR data that meets more than 80 percent but less than 100 percent of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 70 percent but less than or equal to 80 percent of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 60 percent but less than or equal to 70 percent of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets less than or equal to 60 percent of the total recording properties as specified in Requirement R4.
R5	Long-term Planning	Lower	The Reliability Coordinator ~~Responsible Entity~~ identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 80 percent but less than 100 percent of the	The ~~Responsible Entity~~ Reliability Coordinator identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 70 percent but less than or equal to 80 percent of the	The Reliability Coordinator ~~Responsible Entity~~ identified the BES Elements for which DDR data is required as directed by Requirement R5 for more than 60 percent but less than or equal to 70 percent of the	The Reliability Coordinator ~~Responsible Entity~~ identified the BES Elements for which DDR data is required as directed by Requirement R5 for less than or equal to 60 percent of the

			required BES Elements included in Part 5.1. OR The ~~Responsible Entity~~Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by 30-calendar days or less. OR The ~~Responsible Entity~~Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners by 10-calendar days or less.	required BES Elements included in Part 5.1. OR The ~~Responsible Entity~~Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by greater than 30-calendar days and less than or equal to 60 -calendar days. OR The ~~Responsible Entity~~Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners by greater than 10-calendar days but less than or equal to 20-calendar days.	required BES Elements included in Part 5.1. OR The ~~Responsible Entity~~Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by greater than 60-calendar days and less than or equal to 90-calendar days. OR The ~~Responsible Entity~~Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying the owners by greater than 20-calendar days but less than or equal to 30-calendar days.	required BES Elements included in Part 5.1. OR The ~~Responsible Entity~~Reliability Coordinator identified the BES Elements for DDR as directed by Requirement R5, Part 5.1 or Part 5.4 but was late by greater than 90-calendar days. OR The ~~Responsible Entity~~Reliability Coordinator as directed by Requirement R5, Part 5.3 was late in notifying one or more owners by greater than 30-calendar days. OR The ~~Responsible Entity~~Reliability Coordinator failed to ensure a minimum DDR coverage per Part 5.2.

R6	Long-term Planning	Lower	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 that covered more than 80 percent but less than 100 percent of the total required electrical quantities for all applicable BES Elements.	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 70 percent but less than or equal to 80 percent of the total required electrical quantities for all applicable BES Elements.	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 60 percent but less than or equal to 70 percent of the total required electrical quantities for all applicable BES Elements.	The Transmission Owner failed to have DDR data as directed by Requirement R6, Parts 6.1 through 6.4.
R7	Long-term Planning	Lower	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 that covers more than 80 percent but less than 100 percent of the total required electrical quantities for all applicable BES Elements.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 70 percent but less than or equal to 80 percent of the total required electrical quantities for all applicable BES Elements.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 60 percent but less than or equal to 70 percent of the total required electrical quantities for all applicable BES Elements.	The Generator Owner failed to have DDR data as directed by Requirement R7, Parts 7.1 through 7.4.
R8	Long-term Planning	Lower	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed	The Transmission Owner or Generator Owner failed to have continuous or non-continuous DDR data,

			in Requirement R8, for more than 80 percent but less than 100 percent of the BES Elements they own as determined in Requirement R5.	in Requirement R8, for more than 70 percent but less than or equal to 80 percent of the BES Elements they own as determined in Requirement R5.	in Requirement R8, for more than 60 percent but less than or equal to 70 percent of the BES Elements they own as determined in Requirement R5.	as directed in Requirement R8, for the BES Elements they own as determined in Requirement R5.
R9	Long-term Planning	Lower	The Transmission Owner or Generator Owner had DDR data that meets more than 80 percent but less than 100 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets more than 70 percent but less than or equal to 80 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets more than 60 percent but less than or equal to 70 percent of the total recording properties as specified in Requirement R9.	The Transmission Owner or Generator Owner had DDR data that meets less than or equal to 60 percent of the total recording properties as specified in Requirement R9.

R10	Long-term Planning	Lower	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more than 90 percent but less than 100 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more than 80 percent but less than or equal to 90 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.	The Transmission Owner or Generator Owner had time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for more than 70 percent but less than or equal to 80 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.	The Transmission Owner or Generator Owner failed to have time synchronization per Requirement R10, Parts 10.1 and 10.2 for SER, FR, and DDR data for less than or equal to 70 percent of the BES buses identified in Requirement R1 and BES Elements identified in Requirement R5 as directed by Requirement R10.
R11	Long-term Planning	Lower	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 30-calendar days but less than 40-calendar days after the request unless an extension was granted	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 40-calendar days but less than or equal to 50-calendar days after the request unless an extension	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 50-calendar days but less than or equal to 60-calendar days after the request unless an extension	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 failed to provide the requested data more than 60-calendar days after the request unless an extension was granted by the requesting authority.

			by the requesting authority. OR The Transmission Owner or Generator Owner as directed by Requirement R11 provided more than 90 percent but less than 100 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 90 percent of the data but less than 100 percent of the data in the proper data format.	was granted by the requesting authority. OR The Transmission Owner or Generator Owner as directed by Requirement R11 provided more than 80 percent but less than or equal to 90 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 80 percent of the data but less than or equal to 90 percent of the data in the proper data format.	was granted by the requesting authority. OR The Transmission Owner or Generator Owner as directed by Requirement R11 provided more than 70 percent but less than or equal to 80 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 70 percent of the data but less than or equal to 80 percent of the data in the proper data format.	OR The Transmission Owner or Generator Owner as directed by Requirement R11 failed to provide less than or equal to 70 percent of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided less than or equal to 70 percent of the data in the proper data format.
R12	Long-term Planning	Lower	The Transmission Owner or Generator Owner as directed by Requirement R12	The Transmission Owner or Generator Owner as directed by Requirement R12	The Transmission Owner or Generator Owner as directed by Requirement R12	The Transmission Owner or Generator Owner as directed by Requirement R12

			reported a failure and provided a Corrective Action Plan to the Regional Entity more than 90-calendar days but less than or equal to 100-calendar days after discovery of the failure.	reported a failure and provided a Corrective Action Plan to the Regional Entity more than 100-calendar days but less than or equal to 110-calendar days after discovery of the failure.	reported a failure and provided a Corrective Action Plan to the Regional Entity more than 110-calendar days but less than or equal to 120-calendar days after discovery of the failure. OR The Transmission Owner or Generator Owner as directed by Requirement R12 submitted a CAP to the Regional Entity but failed to implement it.	failed to report a failure and provide a Corrective Action Plan to the Regional Entity more than 120-calendar days after discovery of the failure. OR Transmission Owner or Generator Owner as directed by Requirement R12 failed to restore the recording capability and failed to submit a CAP to the Regional Entity.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

G. References

IEEE C37.111: Common format for transient data exchange (COMTRADE) for power Systems.

IEEE C37.232-2011, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME). Standard published 11/09/2011 by IEEE.

NPCC SP6 Report Synchronized Event Data Reporting, revised March 31, 2005

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

U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout in the United States and Canada (Nov. 2003)

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
1	August 2, 2006	Adopted by NERC Board of Trustees	Revised
2	November 13, 2014	Adopted by NERC Board of Trustees	Revised under Project 2007-11 and merged with PRC-018-1.
2	September 24, 2015	FERC approved PRC-005-4. Docket No. RM15-4-000; Order No. 814	

Attachment 1

Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data

(Requirement R1)

To identify monitored BES buses for sequence of events recording (SER) and Fault recording (FR) data required by Requirement 1, each Transmission Owner shall follow sequentially, unless otherwise noted, the steps listed below:

Step 1. Determine a complete list of BES buses that it owns.

For the purposes of this standard, a single BES bus includes physical buses with breakers connected at the same voltage level within the same physical location sharing a common ground grid. These buses may be modeled or represented by a single node in fault studies. For example, ring bus or breaker-and-a-half bus configurations are considered to be a single bus.

Step 2. Reduce the list to those BES buses that have a maximum available calculated three phase short circuit MVA of 1,500 MVA or greater. If there are no buses on the resulting list, proceed to Step 7.

Step 3. Determine the 11 BES buses on the list with the highest maximum available calculated three phase short circuit MVA level. If the list has 11 or fewer buses, proceed to Step 7.

Step 4. Calculate the median MVA level of the 11 BES buses determined in Step 3.

Step 5. Multiply the median MVA level determined in Step 4 by 20 percent.

Step 6. Reduce the BES buses on the list to only those that have a maximum available calculated three phase short circuit MVA higher than the greater of:

- 1,500 MVA or
- 20 percent of median MVA level determined in Step 5.

Step 7. If there are no BES buses on the list: the procedure is complete and no FR and SER data will be required. Proceed to Step 9.

If the list has 1 or more but less than or equal to 11 BES buses: FR and SER data is required at the BES bus with the highest maximum available calculated three phase short circuit MVA as determined in Step 3. Proceed to Step 9.

If the list has more than 11 BES buses: SER and FR data is required on at least the 10 percent of the BES buses determined in Step 6 with the highest maximum available calculated three phase short circuit MVA. Proceed to Step 8.

Step 8. SER and FR data is required at additional BES buses on the list determined in Step 6. The aggregate of the number of BES buses determined in Step 7 and this Step will be at least 20 percent of the BES buses determined in Step 6.

The additional BES buses are selected, at the Transmission Owner's discretion, to provide maximum wide-area coverage for SER and FR data. The following BES bus locations are recommended:

- Electrically distant buses or electrically distant from other DME devices.
- Voltage sensitive areas.
- Cohesive load and generation zones.
- BES buses with a relatively high number of incident Transmission circuits.
- BES buses with reactive power devices.
- Major Facilities interconnecting outside the Transmission Owner's area.

Step 9. The list of monitored BES buses for SER and FR data for Requirement R1 is the aggregate of the BES buses determined in Steps 7 and 8.

Attachment 2

Sequence of Events Recording (SER) Data Format

(Requirement R11, Part 11.3)

Date, Time, Local Time Code, Substation, Device, State[1]

08/27/13, 23:58:57.110, -5, Sub 1, Breaker 1, Close

08/27/13, 23:58:57.082, -5, Sub 2, Breaker 2, Close

08/27/13, 23:58:47.217, -5, Sub 1, Breaker 1, Open

08/27/13, 23:58:47.214, -5, Sub 2, Breaker 2, Open

[1] "OPEN" and "CLOSE" are used as examples. Other terminology such as TRIP, TRIP TO LOCKOUT, RECLOSE, etc. is also acceptable.

High Level Requirement Overview

Requirement	Entity	Identify BES Buses	Notification	SER	FR	5 Year Re-evaluation
R1	TO	X	X	X	X	X
R2	TO | GO			X		
R3	TO | GO				X	
R4	TO | GO				X	

Requirement	Entity	Identify BES Elements	Notification	DDR	5 Year Re-evaluation
R5	~~RE (PC |~~ RC~~)~~	X	X	X	X
R6	TO			X	
R7	GO			X	
R8	TO | GO			X	
R9	TO | GO			X	

Requirement	Entity	Time Synchronization	Provide SER, FR, DDR Data	SER, FR, DDR Availability
R10	TO | GO	X		
R11	TO | GO		X	
R12	TO | GO			X

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 Functional Entities:

~~When the term "Responsible Entity" is used in PRC-002-2, it specifically refers to those entities listed under 4.1. The Responsible Entity – the Planning Coordinator or~~Because the Reliability Coordinator~~, as applicable in each Interconnection –~~ has the best wide-area view of the BES, the Reliability Coordinator ~~and~~ is most suited to be responsible for determining the BES Elements for which dynamic Disturbance recording (DDR) data is required. The Transmission Owners and Generator Owners will have the responsibility for ensuring that adequate data is available for those BES Elements selected.

BES buses where sequence of events recording (SER) and fault recording (FR) data is required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their Systems to determine those buses. The Transmission Owners and Generator Owners that own BES Elements on those BES buses will have the responsibility for ensuring that adequate data is available.

Rationale for R1:

Analysis and reconstruction of BES events requires SER and FR data from key BES buses. Attachment 1 provides a uniform methodology to identify those BES buses. Repeated testing of the Attachment 1 methodology has demonstrated the proper distribution of SER and FR data collection. Review of actual BES short circuit data received from the industry in response to the DMSDT's data request (June 5, 2013 through July 5, 2013) illuminated a strong correlation between the available short circuit MVA at a Transmission bus and its relative size and importance to the BES based on (i) its voltage level, (ii) the number of Transmission Lines and other BES Elements connected to the BES bus, and (iii) the number and size of generating units connected to the bus. BES buses with a large short circuit MVA level are BES Elements that have a significant effect on System reliability and performance. Conversely, BES buses with very low short circuit MVA levels seldom cause wide-area or cascading System events, so SER and FR data from those BES Elements are not as significant. After analyzing and reviewing the collected data submittals from across the continent, the threshold MVA values were chosen to provide sufficient data for event analysis using engineering and operational judgment.

Concerns have existed that the defined methodology for bus selection will overly concentrate data to selected BES buses. For the purpose of PRC-002-2, there are a minimum number of BES buses for which SER and FR data is required based on the short circuit level. With these concepts and the objective being sufficient recording coverage for event analysis, the DMSDT developed the procedure in Attachment 1 that utilizes the maximum available calculated three phase short circuit MVA. This methodology ensures comparable and sufficient coverage for SER and FR data regardless of variations in the size and System topology of Transmission Owners across all Interconnections. Additionally, this methodology provides a degree of flexibility for the use of judgment in the selection process to ensure sufficient distribution.

BES buses where SER and FR data is required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their Systems to determine those buses.

Each Transmission Owner must re-evaluate the list of BES buses at least every five calendar years to address System changes since the previous evaluation. Changes to the BES do not mandate immediate inclusion of BES buses into the currently enforced list, but the list of BES buses will be re-evaluated at least every five calendar years to address System changes since the previous evaluation.

Since there may be multiple owners of equipment that comprise a BES bus, the notification required in R1 is necessary to ensure all owners are notified.

A 90-calendar day notification deadline provides adequate time for the Transmission Owner to make the appropriate determination and notification.

Rationale for R2:
The intent is to capture SER data for the status (open/close) of the circuit breakers that can interrupt the current flow through each BES Element connected to a BES bus. Change of state of circuit breaker position, time stamped according to Requirement R10 to a time synchronized clock, provides the basis for assembling the detailed sequence of events timeline of a power System Disturbance. Other status monitoring nomenclature can be used for devices other than circuit breakers.

Rationale for R3:
The required electrical quantities may either be directly measured or determinable if sufficient FR data is captured (e.g. residual or neutral current if the phase currents are directly measured). In order to cover all possible fault types, all BES bus phase-to-neutral voltages are required to be determinable for each BES bus identified in Requirement R1. BES bus voltage data is adequate for System Disturbance analysis. Phase current and residual current are required to distinguish between phase faults and ground faults. It also facilitates determination of the fault location and cause of relay operation. For transformers (Part 3.2.1), the data may be from either the high-side or the low-side of the transformer. Generator step-up transformers (GSUs) and leads that connect the GSU transformer(s) to the Transmission System that are used exclusively to export energy directly from a BES generating unit or generating plant are excluded from Requirement R3 because the fault current contribution from a generator to a fault on the Transmission System will be captured by FR data on the Transmission System, and Transmission System FR will capture faults on the generator interconnection.

Generator Owners may install this capability or, where the Transmission Owners already have suitable FR data, contract with the Transmission Owner. However, when required, the Generator Owner is still responsible for the provision of this data.

Rationale for R4:
Time stamped pre- and post-trigger fault data aid in the analysis of power System operations and determination if operations were as intended. System faults generally persist for a short time period, thus a 30-cycle total minimum record length is adequate. Multiple records allow for legacy microprocessor relays which, when time-synchronized, are capable of providing adequate fault data but not capable of providing fault data in a single record with 30-contiguous cycles total.

A minimum recording rate of 16 samples per cycle (960 Hz) is required to get sufficient point on wave data for recreating accurate fault conditions.

Rationale for R5:
DDR is used for capturing the BES transient and post-transient response following Disturbances, and the data is used for event analysis and validating System performance. DDR plays a critical role in wide-area Disturbance analysis, and Requirement R5 ensures there is adequate wide-area coverage of DDR data for specific BES Elements to facilitate accurate and efficient event analysis. The Reliability Coordinator~~Responsible Entity~~ has the best wide-area view of the System and needs to ensure that there are sufficient BES Elements identified for DDR data capture. The identification of BES Elements requiring DDR data as per Requirement R5 is based upon industry experience with wide-area Disturbance analysis and the need for adequate data to facilitate event analysis. Ensuring data is captured for these BES Elements will significantly improve the accuracy of analysis and understanding of why an event occurred, not simply what occurred.

From its experience with changes to the Bulk Electric System that would affect DDR, the DMSDT decided that the five calendar year re-evaluation of the list is a reasonable interval for this review. Changes to the BES do not mandate immediate inclusion of BES Elements into the in force list, but the list of BES Elements will be re-evaluated at least every five calendar years to address System changes since the previous evaluation. However, this standard does not preclude the ~~Responsible Entity~~Reliability Coordinator from performing this re-evaluation more frequently to capture updated BES Elements.

~~The Responsible Entity, for the purposes of this standard, is defined as the PC or RC depending upon Interconnection, because they have the best overall perspective for determining wide-area DDR coverage. The Planning Coordinator and Reliability Coordinator assume different functions across the continent; therefore the Responsible Entity is defined in the Applicability Section and used throughout this standard.~~

The ~~Responsible Entity~~Reliability Coordinator must notify all owners of the selected BES Elements that DDR data is required for this standard. The ~~Responsible Entity~~Reliability Coordinator is only required to share the list of selected BES Elements that each Transmission Owner and Generator Owner respectively owns, not the entire list. This communication of selected BES Elements is required to ensure that the owners of the respective BES Elements are aware of their responsibilities under this standard.

Implementation of the monitoring equipment is the responsibility of the respective Transmission Owners and Generator Owners, the timeline for installing this capability is outlined in the Implementation Plan, and starts from notification of the list from the ~~Responsible Entity~~Reliability Coordinator. Data for each BES Element as defined by the ~~Responsible Entity~~Reliability Coordinator must be provided; however, this data can be either directly measured or accurately calculated. With the exception of HVDC circuits, DDR data is only required for one end or terminal of the BES Elements selected. For example, DDR data must be provided for at least one terminal of a Transmission Line or generator step-up (GSU) transformer, but not both terminals. For an interconnection between two ~~Responsible Entities~~Reliability Coordinators, each ~~Responsible Entity~~Reliability Coordinator will consider this interconnection independently, and are expected to work cooperatively to determine how to monitor the BES Elements that require DDR data. For an interconnection between two TO's, or a TO and a GO, the ~~Responsible Entity~~Reliability Coordinator will determine which entity will provide the data. The ~~Responsible Entity~~Reliability Coordinator will notify the owners that their BES Elements require DDR data.

Refer to the Guidelines and Technical Basis Section for more detail on the rationale and technical reasoning for each identified BES Element in Requirement R5, Part 5.1; monitoring these BES Elements with DDR will facilitate thorough and informative event analysis of wide-area Disturbances on the BES. Part 5.2 is included to ensure wide-area coverage across all ~~Responsible Entities~~Reliability Coordinators. It is intended that each ~~Responsible Entity~~Reliability Coordinator will have DDR data for one BES Element and at least one additional BES Element per 3,000 MW of its historical simultaneous peak System Demand.

Rationale for R6:
DDR is used to measure transient response to System Disturbances during a relatively balanced post-fault condition. Therefore, it is sufficient to provide a phase-to-neutral voltage or positive sequence voltage. The electrical quantities can be determined (calculated, derived, etc.).

Because all of the BES buses within a location are at the same frequency, one frequency measurement is adequate.

The data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a BES bus are closed.

Rationale for R7:
A crucial part of wide-area Disturbance analysis is understanding the dynamic response of generating resources. Therefore, it is necessary for Generator Owners to have DDR at either the high- or low-side of the generator step-up transformer (GSU) measuring the specified electrical quantities to adequately capture generator response. This standard defines the 'what' of DDR, not the 'how'. Generator Owners may install this capability or, where the Transmission Owners already have suitable DDR data, contract with the Transmission Owner. However, the Generator Owner is still responsible for the provision of this data.

Rationale for R8:

Large scale System outages generally are an evolving sequence of events that occur over an extended period of time, making DDR data essential for event analysis. Data available pre- and post-contingency helps identify the causes and effects of each event leading to outages. Therefore, continuous recording and storage are necessary to ensure sufficient data is available for the entire event.
Existing DDR data recording across the BES may not record continuously. To accommodate its use for the purposes of this standard, triggered records are acceptable if the equipment was installed prior to the effective date of this standard. The frequency triggers are defined based on the dynamic response associated with each Interconnection. The undervoltage trigger is defined to capture possible delayed undervoltage conditions such as Fault Induced Delayed Voltage Recovery (FIDVR).

Rationale for R9:
An input sampling rate of at least 960 samples per second, which corresponds to 16 samples per cycle on the input side of the DDR equipment, ensures adequate accuracy for calculation of recorded measurements such as complex voltage and frequency.
An output recording rate of electrical quantities of at least 30 times per second refers to the recording and measurement calculation rate of the device. Recorded measurements of at least 30 times per second provide adequate recording speed to monitor the low frequency oscillations typically of interest during power System Disturbances.

Rationale for R10:
Time synchronization of Disturbance monitoring data is essential for time alignment of large volumes of geographically dispersed records from diverse recording sources. Coordinated Universal Time (UTC) is a recognized time standard that utilizes atomic clocks for generating precision time measurements. All data must be provided in UTC formatted time either with or without the local time offset, expressed as a negative number (the difference between UTC and the local time zone where the measurements are recorded).
Accuracy of time synchronization applies only to the clock used for synchronizing the monitoring equipment. The equipment used to measure the electrical quantities must be time synchronized to ± 2 ms accuracy; however, accuracy of the application of this time stamp and therefore the accuracy of the data itself is not mandated. This is because of inherent delays associated with measuring the electrical quantities and events such as breaker closing, measurement transport delays, algorithm and measurement calculation techniques, etc. Ensuring that the monitoring devices internal clocks are within ± 2 ms accuracy will suffice with respect to providing time synchronized data.

Rationale for R11:
Wide-area Disturbance analysis includes data recording from many devices and entities. Standardized formatting and naming conventions of these files significantly improves timely analysis.

Providing the data within 30-calendar days (or the granted extension time), subject to Part 11.1, allows for reasonable time to collect the data and perform any necessary computations or formatting.

Data is required to be retrievable for 10-calendar days inclusive of the day the data was recorded, i.e. a 10-calendar day rolling window of available data. Data hold requests are usually initiated the same or next day following a major event for which data is requested. A 10-calendar day time frame provides a practical limit on the duration of data required to be stored and informs the requesting entities as to how long the data will be available. The requestor of data has to be aware of the Part 11.1 10-calendar day retrievability because requiring data retention for a longer period of time is expensive and unnecessary.

SER data shall be provided in a simple ASCII .CSV format as outlined in Attachment 2. Either equipment can provide the data or a simple conversion program can be used to convert files into this format. This will significantly improve the data format for event records, enabling the use of software tools for analyzing the SER data.

Part 11.4 specifies FR and DDR data files be provided in conformance with IEEE C37.111, IEEE Standard for Common Format for Transient Exchange (COMTRADE), revision 1999 or later. The use of IEEE C37.111-1999 or later is well established in the industry. C37.111-2013 is a version of COMTRADE that includes an annex describing the application of the COMTRADE standard to synchrophasor data; however, version C37.111-1999 is commonly used in the industry today.

Part 11.5 uses a standardized naming format, C37.232-2011, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME), for providing Disturbance monitoring data. This file format allows a streamlined analysis of large Disturbances, and includes critical records such as local time offset associated with the synchronization of the data.

Rationale for R12:
Each Transmission Owner and Generator Owner who owns equipment used for collecting the data required for this standard must repair any failures within 90-calendar days to ensure that adequate data is available for event analysis. If the Disturbance monitoring capability cannot be restored within 90-calendar days (e.g. budget cycle, service crews, vendors, needed outages, etc.), the entity must develop a Corrective Action Plan (CAP) for restoring the data recording capability. The timeline required for the CAP depends on the entity and the type of data required. It is treated as a failure if the recording capability is out of service for maintenance and/or testing for greater than 90-calendar days. An outage of the monitored BES Element does not constitute a failure of the Disturbance monitoring capability.

Guidelines and Technical Basis Section

Introduction

The emphasis of PRC-002-2 is not on how Disturbance monitoring data is captured, but what Bulk Electric System data is captured. There are a variety of ways to capture the data PRC-002-2 addresses, and existing and currently available equipment can meet the requirements of this standard. PRC-002-2 also addresses the importance of addressing the availability of Disturbance monitoring capability to ensure the completeness of BES data capture.

The data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a bus are closed.

PRC-002-2 addresses "what" data is recorded, not "how" it is recorded.

Guideline for Requirement R1:

Sequence of events and fault recording for the analysis, reconstruction, and reporting of System Disturbances is important. However, SER and FR data is not required at every BES bus on the BES to conduct adequate or thorough analysis of a Disturbance. As major tools of event analysis, the time synchronized time stamp for a breaker change of state and the recorded waveforms of voltage and current for individual circuits allows the precise reconstruction of events of both localized and wide-area Disturbances.

More quality information is always better than less when performing event analysis. However, 100 percent coverage of all BES Elements is not practical nor required for effective analysis of wide-area Disturbances. Therefore, selectivity of required BES buses to monitor is important for the following reasons:

1. Identify key BES buses with breakers where crucial information is available when required.
2. Avoid excessive overlap of coverage.
3. Avoid gaps in critical coverage.
4. Provide coverage of BES Elements that could propagate a Disturbance.
5. Avoid mandates to cover BES Elements that are more likely to be a casualty of a Disturbance rather than a cause.
6. Establish selection criteria to provide effective coverage in different regions of the continent.

The major characteristics available to determine the selection process are:

1. System voltage level;
2. The number of Transmission Lines into a substation or switchyard;
3. The number and size of connected generating units;
4. The available short circuit levels.

Although it is straightforward to establish criteria for the application of identified BES buses, analysis was required to establish a sound technical basis to fulfill the required objectives.

To answer these questions and establish criteria for BES buses of SER and FR, the DMSDT established a sub-team referred to as the Monitored Value Analysis Team (MVA Team). The MVA Team collected information from a wide variety of Transmission Systems throughout the continent to analyze Transmission buses by the characteristics previously identified for the selection process.

The MVA Team learned that the development of criteria is not possible for adequate SER and FR coverage, based solely upon simple, bright line characteristics, such as the number of lines into a substation or switchyard at a particular voltage level or at a set level of short circuit current. To provide the appropriate coverage, a relatively simple but effective Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data was developed. This Procedure, included as Attachment 1, assists entities in fulfilling Requirement R1 of the standard.

The Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data is weighted to buses with higher short circuit levels. This is chosen for the following reasons:

1. The method is voltage level independent.
2. It is likely to select buses near large generation centers.
3. It is likely to select buses where delayed clearing can cause Cascading.
4. Selected buses directly correlate to the Universal Power Transfer equation: Lower Impedance – increased power flows – greater System impact.

To perform the calculations of Attachment 1, the following information below is required and the following steps (provided in summary form) are required for Systems with more than 11 BES buses with three phase short circuit levels above 1,500 MVA.

1. Total number of BES buses in the Transmission System under evaluation.
   a. Only tangible substation or switchyard buses are included.
   b. Pseudo buses created for analysis purposes in System models are excluded.
2. Determine the three phase short circuit MVA for each BES bus.
3. Exclude BES buses from the list with short circuit levels below 1,500 MVA.
4. Determine the median short circuit for the top 11 BES buses on the list (position number 6).
5. Multiply median short circuit level by 20 percent.
6. Reduce the list of BES buses to those with short circuit levels higher than 20 percent of the median.
7. Apply SER and FR at BES buses with short circuit levels in the top 10 percent of the list (from 6).

8. Apply SER and FR at BES buses at an additional 10 percent of the list using engineering judgment, and allowing flexibility to factor in the following considerations:
   - Electrically distant BES buses or electrically distant from other DME devices
   - Voltage sensitive areas
   - Cohesive load and generation zones
   - BES buses with a relatively high number of incident Transmission circuits
   - BES buses with reactive power devices
   - Major facilities interconnecting outside the Transmission Owner's area.

For event analysis purposes, more valuable information is attained about generators and their response to System events pre- and post-contingency through DDR data versus SER or FR records. SER data of the opening of the primary generator output interrupting devices (e.g. synchronizing breaker) may not reliably indicate the actual time that a generator tripped; for instance, when it trips on reverse power after loss of its prime mover (e.g. combustion or steam turbine). As a result, this standard only requires DDR data.

The re-evaluation interval of five years was chosen based on the experience of the DMSDT to address changing System configurations while creating balance in the frequency of re-evaluations.

Guideline for Requirement R2:

Analyses of wide-area Disturbances often begin by evaluation of SERs to help determine the initiating event(s) and follow the Disturbance propagation. Recording of breaker operations help determine the interruption of line flows while generator loading is best determined by DDR data, since generator loading can be essentially zero regardless of breaker position. However, generator breakers directly connected to an identified BES bus are required to have SER data captured. It is important in event analysis to know when a BES bus is cleared regardless of a generator's loading.

Generator Owners are included in this requirement because a Generator Owner may, in some instances, own breakers directly connected to the Transmission Owner's BES bus.

Guideline for Requirement R3:

The BES buses for which FR data is required are determined based on the methodology described in Attachment 1 of the standard. The BES Elements connected to those BES buses for which FR data is required include:

- Transformers with a low-side operating voltage of 100kV or above
- Transmission Lines

Only those BES Elements that are identified as BES as defined in the latest in effect NERC definition are to be monitored. For example, radial lines or transformers with low-side voltage less than 100kV are not included.

FR data must be determinable from each terminal of a BES Element connected to applicable BES buses.

Generator step-up transformers (GSU) are excluded from the above based on the following:

- Current contribution from a generator in case of fault on the Transmission System will be captured by FR data on the Transmission System.
- For faults on the interconnection to generating facilities it is sufficient to have fault current data from the Transmission station end of the interconnection. Current contribution from a generator can be readily calculated if needed.

The DMSDT, after consulting with NERC's Event Analysis group, determined that DDR data from selected generator locations was more important for event analysis than FR data.

Recording of Electrical Quantities

For effective fault analysis it is necessary to know values of all phase and neutral currents and all phase-to-neutral voltages. Based on such FR data it is possible to determine all fault types. FR data also augments SERs in evaluating circuit breaker operation.

Current Recordings

The required electrical quantities are normally directly measured. Certain quantities can be derived if sufficient data is measured, for example residual or neutral currents.
Since a Transmission System is generally well balanced, with phase currents having essentially similar magnitudes and phase angle differences of 120°, during normal conditions there is negligible neutral (residual) current. In case of a ground fault the resulting phase current imbalance produces residual current that can be either measured or calculated.

Neutral current, also known as ground or residual current $\mathbf{I}_r$, is calculated as a sum of vectors of three phase currents:

$\mathbf{I}_r = 3 \bullet \mathbf{I}_0 = \mathbf{I}_A + \mathbf{I}_B + \mathbf{I}_C$

$\mathbf{I}_0$ - Zero-sequence current

$\mathbf{I}_A$, $\mathbf{I}_B$, $\mathbf{I}_C$ - Phase current (vectors)

Another example of how required electrical quantities can be derived is based on Kirchhoff's Law. Fault currents for one of the BES Elements connected to a particular BES bus can be derived as a vectorial sum of fault currents recorded at the other BES Elements connected to that BES bus.

Voltage Recordings

Voltages are to be recorded or accurately determined at applicable BES buses.

Guideline for Requirement R4:

Pre- and post-trigger fault data along with the SER breaker data, all time stamped to a common clock at millisecond accuracy, aid in the analysis of protection System operations after a fault to determine if a protection System operated as designed. Generally speaking, BES faults persist for a very short time period, approximately 1 to 30 cycles, thus a 30-cycle record length provides adequate data. Multiple records allow for legacy microprocessor relays which, when time synchronized to a common clock, are capable of providing adequate fault data but not capable of providing fault data in a single record with 30-contiguous cycles total.

A minimum recording rate of 16 samples per cycle is required to get accurate waveforms and to get 1 millisecond resolution for any digital input which may be used for FR.

FR triggers can be set so that when the monitored value on the recording device goes above or below the trigger value, data is recorded. Requirement R4, sub-Part 4.3.1 specifies a neutral (residual) overcurrent trigger for ground faults. Requirement R4, sub-Part 4.3.2 specifies a phase undervoltage or overcurrent trigger for phase-to-phase faults.

Guideline for Requirement R5:

DDR data is used for wide-area Disturbance monitoring to determine the System's electromechanical transient and post-transient response and validate System model performance. DDR is typically located based on strategic studies which include angular, frequency, voltage, and oscillation stability. However, for adequately monitoring the System's dynamic response and ensuring sufficient coverage to determine System performance, DDR is required for key BES Elements in addition to a minimum requirement of DDR coverage.

Each ~~Responsible Entity~~Reliability Coordinator ~~(PC or RC)~~ is required to identify sufficient DDR data capture for, at a minimum, one BES Element and then one additional BES Element per 3,000 MW of historical simultaneous peak System Demand. This DDR data is included to provide adequate System wide coverage across an Interconnection. To clarify, if any of the key BES Elements requiring DDR monitoring are within the ~~Responsible Entity's~~Reliability Coordinator ~~a~~Area, DDR data capability is required. If a ~~Responsible Entity~~Reliability Coordinator ~~(PC or RC)~~ does not meet the requirements of Part 5.1, additional coverage had to be specified.

Loss of large generating resources poses a frequency and angular stability risk for all Interconnections across North America. Data capturing the dynamic response of these machines during a Disturbance helps the analysis of large Disturbances. Having data regarding generator dynamic response to Disturbances greatly improves understanding of ***why*** an event occurs rather than what occurred. To determine and provide the basis for unit size criteria, the DMSDT acquired specific generating unit data from NERC's Generating Availability Data System (GADS) program. The data contained generating unit size information for each generating unit in North America which was reported in 2013 to the NERC GADS program. The DMSDT analyzed

the spreadsheet data to determine: (i) how many units were above or below selected size thresholds; and (ii) the aggregate sum of the ratings of the units within the boundaries of those thresholds. Statistical information about this data was then produced, i.e. averages, means and percentages. The DMSDT determined the following basic information about the generating units of interest (current North America fleet, i.e. units reporting in 2013) included in the spreadsheet:

- The number of individual generating units in total included in the spreadsheet.
- The number of individual generating units rated at 20 MW or larger included in the spreadsheet. These units would generally require that their owners be registered as GOs in the NERC CMEP.
- The total number of units within selected size boundaries.
- The aggregate sum of ratings, in MWs, of the units within the boundaries of those thresholds.

The information in the spreadsheet does not provide information by which the plant information location of each unit can be determined, i.e. the DMSDT could not use the information to determine which units were located together at a given generation site or facility.

From this information, the DMSDT was able to reasonably speculate the generating unit size thresholds proposed in Requirement R5, sub-Part 5.1.1 of the standard. Generating resources intended for DDR data recording are those individual units with gross nameplate ratings "greater than or equal to 500 MVA". The 500 MVA individual unit size threshold was selected because this number roughly accounts for 47 percent of the generating capacity in NERC footprint while only requiring DDR coverage on about 12.5 percent of the generating units. As mentioned, there was no data pertaining to unit location for aggregating plant/facility sizes. However, Requirement R5, sub-Part 5.1.1 is included to capture larger units located at large generating plants which could pose a stability risk to the System if multiple large units were lost due to electrical or non-electrical contingencies. For generating plants, each individual generator at the plant/facility with a gross nameplate rating greater than or equal to 300 MVA must have DDR where the gross nameplate rating of the plant/facility is greater than or equal to 1,000 MVA. The 300 MVA threshold was chosen based on the DMSDT's judgment and experience. The incremental impact to the number of units requiring monitoring is expected to be relatively low. For combined cycle plants where only one generator has a rating greater than or equal to 300MVA, that is the only generator that would need DDR.

Permanent System Operating Limits (SOLs) are used to operate the System within reliable and secure limits. In particular, SOLs related to angular or voltage stability have a significant impact on BES reliability and performance. Therefore, at least one BES Element of an SOL should be monitored.

The draft standard requires "One or more BES Elements that are part of an Interconnection Reliability Operating Limits (IROLs)." Interconnection Reliability Operating Limits (IROLs) are included because the risk of violating these limits poses a risk to System stability and the

potential for cascading outages. IROLs may be defined by a single or multiple monitored BES Element(s) and contingent BES Element(s). The standard does not dictate selection of the contingent and/or monitored BES Elements. Rather the Drafting Team believes this determination is best made by the ~~Responsible Entity~~Reliability Coordinator for each IROL considered based on the severity of violating this IROL.

Locations where an undervoltage load shedding (UVLS) program is deployed are prone to voltage instability since they are generally areas of significant Demand. The ~~Responsible Entity~~Reliability Coordinator ~~(PC or RC)~~ will identify these areas where a UVLS is in service and identify a useful and effective BES Element to monitor for DDR such that action of the UVLS or voltage instability on the BES could be captured. For example, a major 500kV or 230kV substation on the EHV System close to the load pocket where the UVLS is deployed would likely be a valuable electrical location for DDR coverage and would aid in post-Disturbance analysis of the load area's response to large System excursions (voltage, frequency, etc.).

Guideline for Requirement R6:

DDR data shows transient response to System Disturbances after a fault is cleared (post-fault), under a relatively balanced operating condition. Therefore, it is sufficient to provide a single phase-to-neutral voltage or positive sequence voltage. Recording of all three phases of a circuit is not required, although this may be used to compute and record the positive sequence voltage.

The bus where a voltage measurement is required is based on the list of BES Elements defined by the ~~Responsible Entity~~Reliability Coordinator ~~(PC or RC)~~ in Requirement R5. The intent of the standard is not to require a separate voltage measurement of each BES Element where a common bus voltage measurement is available. For example, a breaker-and-a-half or double-bus configuration with a North (or East) Bus and South (or West) Bus, would require both buses to have voltage recording because either can be taken out of service indefinitely with the targeted BES Element remaining in service. This may be accomplished either by recording both bus voltages separately, or by providing a selector switch to connect either of the bus voltage sources to a single recording input of the DDR device. This component of the requirement is therefore included to mitigate the potential of failed frequency, phase angle, real power, and reactive power calculations due to voltage measurements removed from service while sufficient voltage measurement is actually available during these operating conditions.

It must be emphasized that the data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a bus are closed.

When current recording is required, it should be on the same phase as the voltage recording taken at the location if a single phase-to-neutral voltage is provided. Positive sequence current recording is also acceptable.

For all circuits where current recording is required, Real and Reactive Power will be recorded on a three phase basis. These recordings may be derived either from phase quantities or from positive sequence quantities.

Guideline for Requirement R7:

All Guidelines specified for Requirement R6 apply to Requirement R7. Since either the high- or low-side windings of the generator step-up transformer (GSU) may be connected in delta, phase-to-phase voltage recording is an acceptable voltage recording. As was explained in the Guideline for Requirement R6, the BES is operating under a relatively balanced operating condition and, if needed, phase-to-neutral quantities can be derived from phase-to-phase quantities.

Again it must be emphasized that the data requirements for PRC-002-2 are based on a System configuration assuming all normally closed circuit breakers on a bus are closed.

Guideline for Requirement R8:

Wide-area System outages are generally an evolving sequence of events that occur over an extended period of time, making DDR data essential for event analysis. Pre- and post-contingency data helps identify the causes and effects of each event leading to the outages. This drives a need for continuous recording and storage to ensure sufficient data is available for the entire Disturbance.

Transmission Owners and Generator Owners are required to have continuous DDR for the BES Elements identified in Requirement R6. However, this requirement recognizes that legacy equipment may exist for some BES Elements that do not have continuous data recording capabilities. For equipment that was installed prior to the effective date of the standard, triggered DDR records of three minutes are acceptable using at least one of the trigger types specified in Requirement R8, Part 8.2:

- Off nominal frequency triggers are used to capture high- or low-frequency excursions of significant size based on the Interconnection size and inertia.
- Rate of change of frequency triggers are used to capture major changes in System frequency which could be caused by large changes in generation or load, or possibly changes in System impedance.
- The undervoltage trigger specified in this standard is provided to capture possible sustained undervoltage conditions such as Fault Induced Delayed Voltage Recovery (FIDVR) events. A sustained voltage of 85 percent is outside normal schedule operating voltages and is sufficiently low to capture abnormal voltage conditions on the BES.

Guideline for Requirement R9:

DDR data contains the dynamic response of a power System to a Disturbance and is used for analyzing complex power System events. This recording is typically used to capture short-term

and long-term Disturbances, such as a power swing. Since the data of interest is changing over time, DDR data is normally stored in the form of RMS values or phasor values, as opposed to directly sampled data as found in FR data.

The issue of the sampling rate used in a recording instrument is quite important for at least two reasons: the anti-aliasing filter selection and accuracy of signal representation. The anti-aliasing filter selection is associated with the requirement of a sampling rate at least twice the highest frequency of a sampled signal. At the same time, the accuracy of signal representation is also dependent on the selection of the sampling rate. In general, the higher the sampling rate, the better the representation. In the abnormal conditions of interest (e.g. faults or other Disturbances); the input signal may contain frequencies in the range of 0-400 Hz. Hence, the rate of 960 samples per second (16 samples/cycle) is considered an adequate sampling rate that satisfies the input signal requirements.

In general, dynamic events of interest are: inter-area oscillations, local generator oscillations, wind turbine generator torsional modes, HVDC control modes, exciter control modes, and steam turbine torsional modes. Their frequencies range from 0.1-20 Hz. In order to reconstruct these dynamic events, a minimum recording time of 30 times per second is required.

Guideline for Requirement R10: Time synchronization of Disturbance monitoring data allows for the time alignment of large volumes of geographically dispersed data records from diverse recording sources. A universally recognized time standard is necessary to provide the foundation for this alignment. Coordinated Universal Time (UTC) is the foundation used for the time alignment of records. It is an international time standard utilizing atomic clocks for generating precision time measurements at fractions of a second levels. The local time offset, expressed as a negative number, is the difference between UTC and the local time zone where the measurements are recorded.

Accuracy of time synchronization applies only to the clock used for synchronizing the monitoring equipment.

Time synchronization accuracy is specified in response to Recommendation 12b in the NERC August, 2003, Blackout Final NERC Report Section V Conclusions and Recommendations:

“Recommendation 12b: Facilities owners shall, in accordance with regional criteria, upgrade existing dynamic recorders to include GPS time synchronization…”

Also, from the U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout, November 2003, in the United States and Canada, page 103:

“Establishing a precise and accurate sequence of outage-related events was a critical building block for the other parts of the investigation. One of the key problems in developing this sequence was that although much of the data pertinent to an event was time-stamped, there was some variance from source to source in how the time-stamping was done, and not all of the time-stamps were synchronized…”

From NPCC's SP6 Report Synchronized Event Data Reporting, revised March 31, 2005, the investigation by the authoring working group revealed that existing GPS receivers can be expected to provide a time code output which has an uncertainty on the order of 1 millisecond, uncertainty being a quantitative descriptor.

Guideline for Requirement R11:

This requirement directs the applicable entities, upon requests from the ~~Responsible Entity~~Reliability Coordinator, Regional Entity or NERC, to provide SER and FR data for BES buses determined in Requirement R1 and DDR data for BES Elements determined as per Requirement R5. To facilitate the analysis of BES Disturbances, it is important that the data is provided to the requestor within a reasonable period of time.

Requirement R11, Part 11.1 specifies the maximum time frame of 30-calendar days to provide the data. Thirty calendar days is a reasonable time frame to allow for the collection of data, and submission to the requestor. An entity may request an extension of the 30-day submission requirement. If granted by the requestor, the entity must submit the data within the approved extended time.

Requirement R11, Part 11.2 specifies that the minimum time period of 10-calendar days inclusive of the day the data was recorded for which the data will be retrievable. With the equipment in use that has the capability of recording data, having the data retrievable for the 10-calendar days is realistic and doable. It is important to note that applicable entities should account for any expected delays in retrieving data and this may require devices to have data available for more than 10 days. To clarify the 10-calendar day time frame, an incident occurs on Day 1. If a request for data is made on Day 6, then that data has to be provided to the requestor within 30-calendar days after a request or a granted time extension. However, if a request for the data is made on Day 11, that is outside the 10-calendar days specified in the requirement, and an entity would not be out of compliance if it did not have the data.

Requirement R11, Part 11.3 specifies a Comma Separated Value (CSV) format according to Attachment 2 for the SER data. It is necessary to establish a standard format as it will be incorporated with other submitted data to provide a detailed sequence of events timeline of a power System Disturbance.

Requirement R11, Part 11.4 specifies the IEEE C37.111 COMTRADE format for the FR and DDR data. The IEEE C37.111 is the Standard for Common Format for Transient Data Exchange and is well established in the industry. It is necessary to specify a standard format as multiple submissions of data from many sources will be incorporated to provide a detailed analysis of a power System Disturbance. The latest revision of COMTRADE (C37.111-2013) includes an annex describing the application of the COMTRADE standard to synchophasor data.

Requirement R11, Part 11.5 specifies the IEEE C37.232 COMNAME format for naming the data files of the SER, FR and DDR. The IEEE C37.232 is the Standard for Common Format for Naming Time Sequence Data Files. The first version was approved in 2007. From the August 14, 2003 blackout there were thousands of Fault Recording data files collected. The collected data files

did not have a common naming convention and it was therefore difficult to discern which files came from which utilities and which ones were captured by which devices. The lack of a common naming practice seriously hindered the investigation process. Subsequently, and in its initial report on the blackout, NERC stressed the need for having a common naming practice and listed it as one of its top ten recommendations.

Guideline for Requirement R12:

This requirement directs the respective owners of Transmission and Generator equipment to be alert to the proper functioning of equipment used for SER, FR, and DDR data capabilities for the BES buses and BES Elements, which were established in Requirements R1 and R5. The owners are to restore the capability within 90-calendar days of discovery of a failure. This requirement is structured to recognize that the existence of a "reasonable" amount of capability out-of-service does not result in lack of sufficient data for coverage of the System. Furthermore, 90-calendar days is typically sufficient time for repair or maintenance to be performed. However, in recognition of the fact that there may be occasions for which it is not possible to restore the capability within 90-calendar days, the requirement further provides that, for such cases, the entity submit a Corrective Action Plan (CAP) to the Regional Entity and implement it. These actions are considered to be appropriate to provide for robust and adequate data availability.

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 Board of Trustees.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** **Transmission Relay Loadability**

2. **Number:** PRC-023-5

3. **Purpose:** Protective relay settings shall not limit transmission loadability; not interfere with system operators' ability to take remedial action to protect system reliability and; be set to reliably detect all fault conditions and protect the electrical network from these faults.

4. **Applicability:**

   4.1. Functional Entity:

   4.1.1 Transmission Owner with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*.

   4.1.2 Generator Owner with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*.

   4.1.3 Distribution Provider with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*, provided those circuits have bi-directional flow capabilities.

   4.1.4 Planning Coordinator

   4.2. Circuits:

   4.2.1 Circuits Subject to Requirements R1 – R5:

   4.2.1.1 Transmission lines operated at 200 kV and above, except Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

   4.2.1.2 Transmission lines operated at 100 kV to 200 kV selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.3 Transmission lines operated below 100 kV that are part of the BES and selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.4 Transformers with low voltage terminals connected at 200 kV and above.

   4.2.1.5 Transformers with low voltage terminals connected at 100 kV to 200 kV selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.6 Transformers with low voltage terminals connected below 100 kV that are part of the BES and selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.2 Circuits Subject to Requirement R6:

   4.2.2.1 Transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV, except Elements that connect the GSU transformer(s) to the Transmission system that are used

exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

4.2.2.2 Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the BES, except Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

5. Effective Dates: See Implementation Plan for the Revised Definition of "Remedial Action Scheme".

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (Requirement R1, criteria 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*.

Criteria:

1. Set transmission line relays so they do not operate at or below 150% of the highest seasonal Facility Rating of a circuit, for the available defined loading duration nearest 4 hours (expressed in amperes).

2. Set transmission line relays so they do not operate at or below 115% of the highest seasonal 15-minute Facility Rating[1] of a circuit (expressed in amperes).

3. Set transmission line relays so they do not operate at or below 115% of the maximum theoretical power transfer capability (using a 90-degree angle between the sending-end and receiving-end voltages and either reactance or complex impedance) of the circuit (expressed in amperes) using one of the following to perform the power transfer calculation:

- An infinite source (zero source impedance) with a 1.00 per unit bus voltage at each end of the line.
- An impedance at each end of the line, which reflects the actual system source impedance with a 1.05 per unit voltage behind each source impedance.

4. Set transmission line relays on series compensated transmission lines so they do not operate at or below the maximum power transfer capability of the line, determined as the greater of:

- 115% of the highest emergency rating of the series capacitor.
- 115% of the maximum power transfer capability of the circuit (expressed in amperes), calculated in accordance with Requirement R1, criterion 3, using the full line inductive reactance.

[1] When a 15-minute rating has been calculated and published for use in real-time operations, the 15-minute rating can be used to establish the loadability requirement for the protective relays.

5. Set transmission line relays on weak source systems so they do not operate at or below 170% of the maximum end-of-line three-phase fault magnitude (expressed in amperes).

6. Not used.

7. Set transmission line relays applied at the load center terminal, remote from generation stations, so they do not operate at or below 115% of the maximum current flow from the load to the generation source under any system configuration.

8. Set transmission line relays applied on the bulk system-end of transmission lines that serve load remote to the system so they do not operate at or below 115% of the maximum current flow from the system to the load under any system configuration.

9. Set transmission line relays applied on the load-end of transmission lines that serve load remote to the bulk system so they do not operate at or below 115% of the maximum current flow from the load to the system under any system configuration.

10. Set transformer fault protection relays and transmission line relays on transmission lines terminated only with a transformer so that the relays do not operate at or below the greater of:

- 150% of the applicable maximum transformer nameplate rating (expressed in amperes), including the forced cooled ratings corresponding to all installed supplemental cooling equipment.
- 115% of the highest operator established emergency transformer rating.

10.1 Set load-responsive transformer fault protection relays, if used, such that the protection settings do not expose the transformer to a fault level and duration that exceeds the transformer's mechanical withstand capability[2].

11. For transformer overload protection relays that do not comply with the loadability component of Requirement R1, criterion 10 set the relays according to one of the following:

- Set the relays to allow the transformer to be operated at an overload level of at least 150% of the maximum applicable nameplate rating, or 115% of the highest operator established emergency transformer rating, whichever is greater, for at least 15 minutes to provide time for the operator to take controlled action to relieve the overload.
- Install supervision for the relays using either a top oil or simulated winding hot spot temperature element set no less than 100° C for the top oil temperature or no less than 140° C for the winding hot spot temperature[3].

12. When the desired transmission line capability is limited by the requirement to adequately protect the transmission line, set the transmission line distance relays to a maximum of 125% of the apparent impedance (at the impedance angle of the transmission line) subject to the following constraints:

a. Set the maximum torque angle (MTA) to 90 degrees or the highest supported by the manufacturer.

---

[2] As illustrated by the "dotted line" in IEEE C57.109-1993 - *IEEE Guide for Liquid-Immersed Transformer Through-Fault-Current Duration*, Clause 4.4, Figure 4.

[3] IEEE standard C57.91, Tables 7 and 8, specify that transformers are to be designed to withstand a winding hot spot temperature of 180 degrees C, and Annex A cautions that bubble formation may occur above 140 degrees C.

b. Evaluate the relay loadability in amperes at the relay trip point at 0.85 per unit voltage and a power factor angle of 30 degrees.

c. Include a relay setting component of 87% of the current calculated in Requirement R1, criterion 12 in the Facility Rating determination for the circuit.

13. Where other situations present practical limitations on circuit capability, set the phase protection relays so they do not operate at or below 115% of such limitations.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider shall set its out-of-step blocking elements to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that uses a circuit capability with the practical limitations described in Requirement R1, criterion 7, 8, 9, 12, or 13 shall use the calculated circuit capability as the Facility Rating of the circuit and shall obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that chooses to use Requirement R1 criterion 2 as the basis for verifying transmission line relay loadability shall provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays at least once each calendar year, with no more than 15 months between reports. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that sets transmission line relays according to Requirement R1 criterion 12 shall provide an updated list of the circuits associated with those relays to its Regional Entity at least once each calendar year, with no more than 15 months between reports, to allow the ERO to compile a list of all circuits that have protective relay settings that limit circuit capability. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

R6. Each Planning Coordinator shall conduct an assessment at least once each calendar year, with no more than 15 months between assessments, by applying the criteria in PRC-023-4, Attachment B to determine the circuits in its Planning Coordinator area for which Transmission Owners, Generator Owners, and Distribution Providers must comply with Requirements R1 through R5. The Planning Coordinator shall: *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

6.1 Maintain a list of circuits subject to PRC-023-4 per application of Attachment B, including identification of the first calendar year in which any criterion in PRC-023-4, Attachment B applies.

6.2 Provide the list of circuits to all Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within 30 calendar days of the establishment of the initial list and within 30 calendar days of any changes to that list.

C. Measures

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its transmission relays is

set according to one of the criteria in Requirement R1, criterion 1 through 13 and shall have evidence such as coordination curves or summaries of calculations that show that relays set per criterion 10 do not expose the transformer to fault levels and durations beyond those indicated in the standard. (R1)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its out-of-step blocking elements is set to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. (R2)

M3. Each Transmission Owner, Generator Owner, and Distribution Provider with transmission relays set according to Requirement R1, criterion 7, 8, 9, 12, or 13 shall have evidence such as Facility Rating spreadsheets or Facility Rating database to show that it used the calculated circuit capability as the Facility Rating of the circuit and evidence such as dated correspondence that the resulting Facility Rating was agreed to by its associated Planning Coordinator, Transmission Operator, and Reliability Coordinator. (R3)

M4. Each Transmission Owner, Generator Owner, or Distribution Provider that sets transmission line relays according to Requirement R1, criterion 2 shall have evidence such as dated correspondence to show that it provided its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays within the required timeframe. The updated list may either be a full list, a list of incremental changes to the previous list, or a statement that there are no changes to the previous list. (R4)

M5. Each Transmission Owner, Generator Owner, or Distribution Provider that sets transmission line relays according to Requirement R1, criterion 12 shall have evidence such as dated correspondence that it provided an updated list of the circuits associated with those relays to its Regional Entity within the required timeframe. The updated list may either be a full list, a list of incremental changes to the previous list, or a statement that there are no changes to the previous list. (R5)

M6. Each Planning Coordinator shall have evidence such as power flow results, calculation summaries, or study reports that it used the criteria established within PRC-023-4, Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard as described in Requirement R6. The Planning Coordinator shall have a dated list of such circuits and shall have evidence such as dated correspondence that it provided the list to the Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within the required timeframe. (R6)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Data Retention

The Transmission Owner, Generator Owner, Distribution Provider and Planning Coordinator 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 Owner, Generator Owner, and Distribution Provider shall each retain documentation to demonstrate compliance with Requirements R1 through R5 for three calendar years.

The Planning Coordinator shall retain documentation of the most recent review process required in Requirement R6. The Planning Coordinator shall retain the most recent list of circuits in its Planning Coordinator area for which applicable entities must comply with the standard, as determined per Requirement R6.

If a Transmission Owner, Generator Owner, Distribution Provider, or Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Violation Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None.

2. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	N/A	N/A	N/A	The responsible entity did not use any one of the following criteria (Requirement R1 criterion 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. OR The responsible entity did not evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees.
R2	N/A	N/A	N/A	The responsible entity failed to ensure that its out-of-step blocking elements allowed tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1.
R3	N/A	N/A	N/A	The responsible entity that uses a circuit capability with the practical limitations described in Requirement R1 criterion 7, 8, 9, 12, or 13 did not use the calculated circuit capability as the Facility Rating of the circuit.

Requirement	Lower	Moderate	High	Severe
				OR The responsible entity did not obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability.
R4	N/A	N/A	N/A	The responsible entity did not provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 2 at least once each calendar year, with no more than 15 months between reports.
R5	N/A	N/A	N/A	The responsible entity did not provide its Regional Entity, with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 12 at least once each calendar year, with no more than 15 months between reports.
R6	N/A	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but more	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but 24	The Planning Coordinator failed to use the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard.

Requirement	Lower	Moderate	High	Severe
		than 15 months and less than 24 months lapsed between assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but failed to include the calendar year in which any criterion in Attachment B first applies. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 31 days and 45 days after	months or more lapsed between assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 46 days and 60 days after list was established or updated. (part 6.2)	OR The Planning Coordinator used the criteria established within Attachment B, at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to meet parts 6.1 and 6.2. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to maintain the list of circuits determined according to the process described in Requirement R6. (part 6.1) OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met

Requirement	Lower	Moderate	High	Severe
		the list was established or updated. (part 6.2)		6.1 but failed to provide the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area or provided the list more than 60 days after the list was established or updated. (part 6.2) OR The Planning Coordinator failed to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard.

E. Regional Differences

None.

F. Supplemental Technical Reference Document

1. The following document is an explanatory supplement to the standard. It provides the technical rationale underlying the requirements in this standard. The reference document contains methodology examples for illustration purposes it does not preclude other technically comparable methodologies.

"Determination and Application of Practical Relaying Loadability Ratings," Version 1.0, June 2008, prepared by the System Protection and Control Task Force of the NERC Planning Committee, available at: http://www.nerc.com/fileUploads/File/Standards/Relay_Loadability_Reference_Doc_Clean_Final_2008July3.pdf

Version History

Version	Date	Action	Change Tracking
1	February 12, 2008	Approved by Board of Trustees	New
1	March 19, 2008	Corrected typo in last sentence of Severe VSL for Requirement 3 — "then" should be "than."	Errata
1	March 18, 2010	Approved by FERC	
1	Filed for approval April 19, 2010	Changed VRF for R3 from Medium to High; changed VSLs for R1, R2, R3 to binary Severe to comply with Order 733	Revision
2	March 10, 2011 approved by Board of Trustees	Revised to address initial set of directives from Order 733	Revision (Project 2010-13)
2	March 15, 2012	FERC order issued approving PRC-023-2 (approval becomes effective May 7, 2012)	
3	November 7, 2013	Adopted by NERC Board of Trustees	Supplemental SAR to Clarify applicability for consistency with PRC-025-1 and other minor corrections.

Version	Date	Action	Change Tracking
4	November 13, 2014	Adopted by the NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
4	November 19, 2015	FERC Order issued approving PRC-023-4. Docket No. RM15-13-000.	

PRC-023-4 — Attachment A

1. This standard includes any protective functions which could trip with or without time delay, on load current, including but not limited to:

1.1. Phase distance.

1.2. Out-of-step tripping.

1.3. Switch-on-to-fault.

1.4. Overcurrent relays.

1.5. Communications aided protection schemes including but not limited to:

1.5.1 Permissive overreach transfer trip (POTT).

1.5.2 Permissive under-reach transfer trip (PUTT).

1.5.3 Directional comparison blocking (DCB).

1.5.4 Directional comparison unblocking (DCUB).

1.6. Phase overcurrent supervisory elements (i.e., phase fault detectors) associated with current-based, communication-assisted schemes (i.e., pilot wire, phase comparison, and line current differential) where the scheme is capable of tripping for loss of communications.

2. The following protection systems are excluded from requirements of this standard:

2.1. Relay elements that are only enabled when other relays or associated systems fail. For example:

- Overcurrent elements that are only enabled during loss of potential conditions.
- Elements that are only enabled during a loss of communications except as noted in section 1.6.

2.2. Protection systems intended for the detection of ground fault conditions.

2.3. Protection systems intended for protection during stable power swings.

2.4. Not used.

2.5. Relay elements used only for Remedial Action Schemes applied and approved in accordance with NERC Reliability Standards PRC-012 through PRC-017 or their successors.

2.6. Protection systems that are designed only to respond in time periods which allow 15 minutes or greater to respond to overload conditions.

2.7. Thermal emulation relays which are used in conjunction with dynamic Facility Ratings.

2.8. Relay elements associated with dc lines.

2.9. Relay elements associated with dc converter transformers.

PRC-023-4 — Attachment B

Circuits to Evaluate

- Transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV.
- Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the Bulk Electric System.

Criteria

If any of the following criteria apply to a circuit, the applicable entity must comply with the standard for that circuit.

B1. The circuit is a monitored Facility of a permanent flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection as defined by the Regional Entity, or a comparable monitored Facility in the Québec Interconnection, that has been included to address reliability concerns for loading of that circuit, as confirmed by the applicable Planning Coordinator.

B2. The circuit is selected by the Planning Coordinator based on Planning Assessments that identify instances of instability, Cascading, or uncontrolled separation.

B3. The circuit forms a path (as agreed to by the Generator Operator and the transmission entity) to supply off-site power to a nuclear plant as established in the Nuclear Plant Interface Requirements (NPIRs) pursuant to NUC-001.

B4. The circuit is identified through the following sequence of power flow analyses[4] performed by the Planning Coordinator for the one-to-five-year planning horizon:

a. Simulate double contingency combinations selected by engineering judgment, without manual system adjustments in between the two contingencies (reflects a situation where a System Operator may not have time between the two contingencies to make appropriate system adjustments).

b. For circuits operated between 100 kV and 200 kV evaluate the post-contingency loading, in consultation with the Facility owner, against a threshold based on the Facility Rating assigned for that circuit and used in the power flow case by the Planning Coordinator.

c. When more than one Facility Rating for that circuit is available in the power flow case, the threshold for selection will be based on the Facility Rating for the loading duration nearest four hours.

[4] Past analyses may be used to support the assessment if no material changes to the system have occurred since the last assessment

d. The threshold for selection of the circuit will vary based on the loading duration assumed in the development of the Facility Rating.

   i. If the Facility Rating is based on a loading duration of up to and including four hours, the circuit must comply with the standard if the loading exceeds 115% of the Facility Rating.

   ii. If the Facility Rating is based on a loading duration greater than four and up to and including eight hours, the circuit must comply with the standard if the loading exceeds 120% of the Facility Rating.

   iii. If the Facility Rating is based on a loading duration of greater than eight hours, the circuit must comply with the standard if the loading exceeds 130% of the Facility Rating.

e. Radially operated circuits serving only load are excluded.

B5. The circuit is selected by the Planning Coordinator based on technical studies or assessments, other than those specified in criteria B1 through B4, in consultation with the Facility owner.

B6. The circuit is mutually agreed upon for inclusion by the Planning Coordinator and the Facility owner.

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 Board of Trustees.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	August 2018 – September 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** **Transmission Relay Loadability**

2. **Number:** PRC-023-54

3. **Purpose:** Protective relay settings shall not limit transmission loadability; not interfere with system operators' ability to take remedial action to protect system reliability and; be set to reliably detect all fault conditions and protect the electrical network from these faults.

4. **Applicability:**

   4.1. Functional Entity:

   4.1.1 Transmission Owner with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*.

   4.1.2 Generator Owner with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*.

   4.1.3 Distribution Provider with load-responsive phase protection systems as described in PRC-023-4 - Attachment A, applied at the terminals of the circuits defined in 4.2.1 *(Circuits Subject to Requirements R1 – R5)*, provided those circuits have bi-directional flow capabilities.

   4.1.4 Planning Coordinator

   4.2. Circuits:

   4.2.1 Circuits Subject to Requirements R1 – R5:

   4.2.1.1 Transmission lines operated at 200 kV and above, except Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

   4.2.1.2 Transmission lines operated at 100 kV to 200 kV selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.3 Transmission lines operated below 100 kV that are part of the BES and selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.4 Transformers with low voltage terminals connected at 200 kV and above.

   4.2.1.5 Transformers with low voltage terminals connected at 100 kV to 200 kV selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.1.6 Transformers with low voltage terminals connected below 100 kV that are part of the BES and selected by the Planning Coordinator in accordance with Requirement R6.

   4.2.2 Circuits Subject to Requirement R6:

   4.2.2.1 Transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV, except Elements that connect the GSU transformer(s) to the Transmission system that are used

exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

4.2.2.2 Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the BES, except Elements that connect the GSU transformer(s) to the Transmission system that are used exclusively to export energy directly from a BES generating unit or generating plant. Elements may also supply generating plant loads.

5. Effective Dates: See Implementation Plan for the Revised Definition of "Remedial Action Scheme".

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (Requirement R1, criteria 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*.

Criteria:

1. Set transmission line relays so they do not operate at or below 150% of the highest seasonal Facility Rating of a circuit, for the available defined loading duration nearest 4 hours (expressed in amperes).

2. Set transmission line relays so they do not operate at or below 115% of the highest seasonal 15-minute Facility Rating[1] of a circuit (expressed in amperes).

3. Set transmission line relays so they do not operate at or below 115% of the maximum theoretical power transfer capability (using a 90-degree angle between the sending-end and receiving-end voltages and either reactance or complex impedance) of the circuit (expressed in amperes) using one of the following to perform the power transfer calculation:

- An infinite source (zero source impedance) with a 1.00 per unit bus voltage at each end of the line.
- An impedance at each end of the line, which reflects the actual system source impedance with a 1.05 per unit voltage behind each source impedance.

4. Set transmission line relays on series compensated transmission lines so they do not operate at or below the maximum power transfer capability of the line, determined as the greater of:

- 115% of the highest emergency rating of the series capacitor.
- 115% of the maximum power transfer capability of the circuit (expressed in amperes), calculated in accordance with Requirement R1, criterion 3, using the full line inductive reactance.

[1] When a 15-minute rating has been calculated and published for use in real-time operations, the 15-minute rating can be used to establish the loadability requirement for the protective relays.

5. Set transmission line relays on weak source systems so they do not operate at or below 170% of the maximum end-of-line three-phase fault magnitude (expressed in amperes).

6. Not used.

7. Set transmission line relays applied at the load center terminal, remote from generation stations, so they do not operate at or below 115% of the maximum current flow from the load to the generation source under any system configuration.

8. Set transmission line relays applied on the bulk system-end of transmission lines that serve load remote to the system so they do not operate at or below 115% of the maximum current flow from the system to the load under any system configuration.

9. Set transmission line relays applied on the load-end of transmission lines that serve load remote to the bulk system so they do not operate at or below 115% of the maximum current flow from the load to the system under any system configuration.

10. Set transformer fault protection relays and transmission line relays on transmission lines terminated only with a transformer so that the relays do not operate at or below the greater of:

- 150% of the applicable maximum transformer nameplate rating (expressed in amperes), including the forced cooled ratings corresponding to all installed supplemental cooling equipment.
- 115% of the highest operator established emergency transformer rating.

10.1 Set load-responsive transformer fault protection relays, if used, such that the protection settings do not expose the transformer to a fault level and duration that exceeds the transformer's mechanical withstand capability[2].

11. For transformer overload protection relays that do not comply with the loadability component of Requirement R1, criterion 10 set the relays according to one of the following:

- Set the relays to allow the transformer to be operated at an overload level of at least 150% of the maximum applicable nameplate rating, or 115% of the highest operator established emergency transformer rating, whichever is greater, for at least 15 minutes to provide time for the operator to take controlled action to relieve the overload.
- Install supervision for the relays using either a top oil or simulated winding hot spot temperature element set no less than 100° C for the top oil temperature or no less than 140° C for the winding hot spot temperature[3].

12. When the desired transmission line capability is limited by the requirement to adequately protect the transmission line, set the transmission line distance relays to a maximum of 125% of the apparent impedance (at the impedance angle of the transmission line) subject to the following constraints:

a. Set the maximum torque angle (MTA) to 90 degrees or the highest supported by the manufacturer.

---

[2] As illustrated by the "dotted line" in IEEE C57.109-1993 - *IEEE Guide for Liquid-Immersed Transformer Through-Fault-Current Duration*, Clause 4.4, Figure 4.

[3] IEEE standard C57.91, Tables 7 and 8, specify that transformers are to be designed to withstand a winding hot spot temperature of 180 degrees C, and Annex A cautions that bubble formation may occur above 140 degrees C.

b. Evaluate the relay loadability in amperes at the relay trip point at 0.85 per unit voltage and a power factor angle of 30 degrees.

c. Include a relay setting component of 87% of the current calculated in Requirement R1, criterion 12 in the Facility Rating determination for the circuit.

13. Where other situations present practical limitations on circuit capability, set the phase protection relays so they do not operate at or below 115% of such limitations.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider shall set its out-of-step blocking elements to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that uses a circuit capability with the practical limitations described in Requirement R1, criterion 7, 8, 9, 12, or 13 shall use the calculated circuit capability as the Facility Rating of the circuit and shall obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that chooses to use Requirement R1 criterion 2 as the basis for verifying transmission line relay loadability shall provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays at least once each calendar year, with no more than 15 months between reports. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that sets transmission line relays according to Requirement R1 criterion 12 shall provide an updated list of the circuits associated with those relays to its Regional Entity at least once each calendar year, with no more than 15 months between reports, to allow the ERO to compile a list of all circuits that have protective relay settings that limit circuit capability. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

R6. Each Planning Coordinator shall conduct an assessment at least once each calendar year, with no more than 15 months between assessments, by applying the criteria in PRC-023-4, Attachment B to determine the circuits in its Planning Coordinator area for which Transmission Owners, Generator Owners, and Distribution Providers must comply with Requirements R1 through R5. The Planning Coordinator shall: *[Violation Risk Factor: High] [Time Horizon: Long Term Planning]*

6.1 Maintain a list of circuits subject to PRC-023-4 per application of Attachment B, including identification of the first calendar year in which any criterion in PRC-023-4, Attachment B applies.

6.2 Provide the list of circuits to all Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within 30 calendar days of the establishment of the initial list and within 30 calendar days of any changes to that list.

C. Measures

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its transmission relays is

set according to one of the criteria in Requirement R1, criterion 1 through 13 and shall have evidence such as coordination curves or summaries of calculations that show that relays set per criterion 10 do not expose the transformer to fault levels and durations beyond those indicated in the standard. (R1)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its out-of-step blocking elements is set to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. (R2)

M3. Each Transmission Owner, Generator Owner, and Distribution Provider with transmission relays set according to Requirement R1, criterion 7, 8, 9, 12, or 13 shall have evidence such as Facility Rating spreadsheets or Facility Rating database to show that it used the calculated circuit capability as the Facility Rating of the circuit and evidence such as dated correspondence that the resulting Facility Rating was agreed to by its associated Planning Coordinator, Transmission Operator, and Reliability Coordinator. (R3)

M4. Each Transmission Owner, Generator Owner, or Distribution Provider that sets transmission line relays according to Requirement R1, criterion 2 shall have evidence such as dated correspondence to show that it provided its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays within the required timeframe. The updated list may either be a full list, a list of incremental changes to the previous list, or a statement that there are no changes to the previous list. (R4)

M5. Each Transmission Owner, Generator Owner, or Distribution Provider that sets transmission line relays according to Requirement R1, criterion 12 shall have evidence such as dated correspondence that it provided an updated list of the circuits associated with those relays to its Regional Entity within the required timeframe. The updated list may either be a full list, a list of incremental changes to the previous list, or a statement that there are no changes to the previous list. (R5)

M6. Each Planning Coordinator shall have evidence such as power flow results, calculation summaries, or study reports that it used the criteria established within PRC-023-4, Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard as described in Requirement R6. The Planning Coordinator shall have a dated list of such circuits and shall have evidence such as dated correspondence that it provided the list to the Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within the required timeframe. (R6)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Data Retention

The Transmission Owner, Generator Owner, Distribution Provider and Planning Coordinator 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 Owner, Generator Owner, and Distribution Provider shall each retain documentation to demonstrate compliance with Requirements R1 through R5 for three calendar years.

The Planning Coordinator shall retain documentation of the most recent review process required in Requirement R6. The Planning Coordinator shall retain the most recent list of circuits in its Planning Coordinator area for which applicable entities must comply with the standard, as determined per Requirement R6.

If a Transmission Owner, Generator Owner, Distribution Provider, or Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Violation Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None.

2. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	N/A	N/A	N/A	The responsible entity did not use any one of the following criteria (Requirement R1 criterion 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. OR The responsible entity did not evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees.
R2	N/A	N/A	N/A	The responsible entity failed to ensure that its out-of-step blocking elements allowed tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1.
R3	N/A	N/A	N/A	The responsible entity that uses a circuit capability with the practical limitations described in Requirement R1 criterion 7, 8, 9, 12, or 13 did not use the calculated circuit capability as the Facility Rating of the circuit.

Requirement	Lower	Moderate	High	Severe
				OR The responsible entity did not obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability.
R4	N/A	N/A	N/A	The responsible entity did not provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 2 at least once each calendar year, with no more than 15 months between reports.
R5	N/A	N/A	N/A	The responsible entity did not provide its Regional Entity, with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 12 at least once each calendar year, with no more than 15 months between reports.
R6	N/A	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but more	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but 24	The Planning Coordinator failed to use the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard.

Requirement	Lower	Moderate	High	Severe
		than 15 months and less than 24 months lapsed between assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but failed to include the calendar year in which any criterion in Attachment B first applies. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 31 days and 45 days after	months or more lapsed between assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 46 days and 60 days after list was established or updated. (part 6.2)	OR The Planning Coordinator used the criteria established within Attachment B, at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to meet parts 6.1 and 6.2. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to maintain the list of circuits determined according to the process described in Requirement R6. (part 6.1) OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met

Requirement	Lower	Moderate	High	Severe
		the list was established or updated. (part 6.2)		6.1 but failed to provide the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area or provided the list more than 60 days after the list was established or updated. (part 6.2) OR The Planning Coordinator failed to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard.

E. Regional Differences

None.

F. Supplemental Technical Reference Document

1. The following document is an explanatory supplement to the standard. It provides the technical rationale underlying the requirements in this standard. The reference document contains methodology examples for illustration purposes it does not preclude other technically comparable methodologies.

"Determination and Application of Practical Relaying Loadability Ratings," Version 1.0, June 2008, prepared by the System Protection and Control Task Force of the NERC Planning Committee, available at: http://www.nerc.com/fileUploads/File/Standards/Relay_Loadability_Reference_Doc_Clean_Final_2008July3.pdf

Version History

Version	Date	Action	Change Tracking
1	February 12, 2008	Approved by Board of Trustees	New
1	March 19, 2008	Corrected typo in last sentence of Severe VSL for Requirement 3 — "then" should be "than."	Errata
1	March 18, 2010	Approved by FERC	
1	Filed for approval April 19, 2010	Changed VRF for R3 from Medium to High; changed VSLs for R1, R2, R3 to binary Severe to comply with Order 733	Revision
2	March 10, 2011 approved by Board of Trustees	Revised to address initial set of directives from Order 733	Revision (Project 2010-13)
2	March 15, 2012	FERC order issued approving PRC-023-2 (approval becomes effective May 7, 2012)	
3	November 7, 2013	Adopted by NERC Board of Trustees	Supplemental SAR to Clarify applicability for consistency with PRC-025-1 and other minor corrections.

Version	Date	Action	Change Tracking
4	November 13, 2014	Adopted by the NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
4	November 19, 2015	FERC Order issued approving PRC-023-4. Docket No. RM15-13-000.	

PRC-023-4 — Attachment A

1. This standard includes any protective functions which could trip with or without time delay, on load current, including but not limited to:

1.1. Phase distance.

1.2. Out-of-step tripping.

1.3. Switch-on-to-fault.

1.4. Overcurrent relays.

1.5. Communications aided protection schemes including but not limited to:

1.5.1 Permissive overreach transfer trip (POTT).

1.5.2 Permissive under-reach transfer trip (PUTT).

1.5.3 Directional comparison blocking (DCB).

1.5.4 Directional comparison unblocking (DCUB).

1.6. Phase overcurrent supervisory elements (i.e., phase fault detectors) associated with current-based, communication-assisted schemes (i.e., pilot wire, phase comparison, and line current differential) where the scheme is capable of tripping for loss of communications.

2. The following protection systems are excluded from requirements of this standard:

2.1. Relay elements that are only enabled when other relays or associated systems fail. For example:

- Overcurrent elements that are only enabled during loss of potential conditions.
- Elements that are only enabled during a loss of communications except as noted in section 1.6.

2.2. Protection systems intended for the detection of ground fault conditions.

2.3. Protection systems intended for protection during stable power swings.

2.4. Not used.

2.5. Relay elements used only for Remedial Action Schemes applied and approved in accordance with NERC Reliability Standards PRC-012 through PRC-017 or their successors.

2.6. Protection systems that are designed only to respond in time periods which allow 15 minutes or greater to respond to overload conditions.

2.7. Thermal emulation relays which are used in conjunction with dynamic Facility Ratings.

2.8. Relay elements associated with dc lines.

2.9. Relay elements associated with dc converter transformers.

PRC-023-4 — Attachment B

Circuits to Evaluate

- Transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV.
- Transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are part of the Bulk Electric System.

Criteria

If any of the following criteria apply to a circuit, the applicable entity must comply with the standard for that circuit.

B1. The circuit is a monitored Facility of a permanent flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection as defined by the Regional Entity, or a comparable monitored Facility in the Québec Interconnection, that has been included to address reliability concerns for loading of that circuit, as confirmed by the applicable Planning Coordinator.

B2. The circuit is selected by the Planning Coordinator based on Planning Assessments that identify instances of instability, Cascading, or uncontrolled separation.

~~**B2.** The circuit is a monitored Facility of an Interconnection Reliability Operating Limit (IROL), where the IROL was determined in the planning horizon pursuant to FAC-010.~~

B3. The circuit forms a path (as agreed to by the Generator Operator and the transmission entity) to supply off-site power to a nuclear plant as established in the Nuclear Plant Interface Requirements (NPIRs) pursuant to NUC-001.

B4. The circuit is identified through the following sequence of power flow analyses[4] performed by the Planning Coordinator for the one-to-five-year planning horizon:

a. Simulate double contingency combinations selected by engineering judgment, without manual system adjustments in between the two contingencies (reflects a situation where a System Operator may not have time between the two contingencies to make appropriate system adjustments).

b. For circuits operated between 100 kV and 200 kV evaluate the post-contingency loading, in consultation with the Facility owner, against a threshold based on the Facility Rating assigned for that circuit and used in the power flow case by the Planning Coordinator.

[4] Past analyses may be used to support the assessment if no material changes to the system have occurred since the last assessment

c. When more than one Facility Rating for that circuit is available in the power flow case, the threshold for selection will be based on the Facility Rating for the loading duration nearest four hours.

d. The threshold for selection of the circuit will vary based on the loading duration assumed in the development of the Facility Rating.

   i. If the Facility Rating is based on a loading duration of up to and including four hours, the circuit must comply with the standard if the loading exceeds 115% of the Facility Rating.

   ii. If the Facility Rating is based on a loading duration greater than four and up to and including eight hours, the circuit must comply with the standard if the loading exceeds 120% of the Facility Rating.

   iii. If the Facility Rating is based on a loading duration of greater than eight hours, the circuit must comply with the standard if the loading exceeds 130% of the Facility Rating.

e. Radially operated circuits serving only load are excluded.

B5. The circuit is selected by the Planning Coordinator based on technical studies or assessments, other than those specified in criteria B1 through B4, in consultation with the Facility owner.

B6. The circuit is mutually agreed upon for inclusion by the Planning Coordinator and the Facility owner.

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 Board of Trustees.

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	June 2018 – July 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** **Relay Performance During Stable Power Swings**

2. **Number:** **PRC-026-2**

3. **Purpose:** To ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Generator Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.1.2 Planning Coordinator.

   4.1.3 Transmission Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.2. Facilities: The following Elements that are part of the Bulk Electric System (BES):

   4.2.1 Generators.

   4.2.2 Transformers.

   4.2.3 Transmission lines.

5. **Background:**

   This is the third phase of a three-phased standard development project that focused on developing this new Reliability Standard to address protective relay operations due to stable power swings. The March 18, 2010, Federal Energy Regulatory Commission (FERC) Order No. 733 approved Reliability Standard PRC-023-1 – Transmission Relay Loadability. In that Order, FERC directed NERC to address three areas of relay loadability that include modifications to the approved PRC-023-1, development of a new Reliability Standard to address generator protective relay loadability, and a new Reliability Standard to address the operation of protective relays due to stable power swings. This project's SAR addresses these directives with a three-phased approach to standard development.

   Phase 1 focused on making the specific modifications from FERC Order No. 733 to PRC-023-1. Reliability Standard PRC-023-2, which incorporated these modifications, became mandatory on July 1, 2012.

   Phase 2 focused on developing a new Reliability Standard, PRC-025-1 – Generator Relay Loadability, to address generator protective relay loadability. PRC-025-1 became mandatory on October 1, 2014, along with PRC-023-3, which was modified to harmonize PRC-023-2 with PRC-025-1.

   Phase 3 focuses on preventing protective relays from tripping unnecessarily due to stable power swings by requiring identification of Elements on which a stable or unstable power

swing may affect Protection System operation, assessment of the security of load-responsive protective relays to tripping in response to only a stable power swing, and implementation of Corrective Action Plans (CAP), where necessary. Phase 3 improves security of load-responsive protective relays for stable power swings so they are expected to not trip in response to stable power swings during non-Fault conditions while maintaining dependable fault detection and dependable out-of-step tripping.

6. Effective Dates:

Requirement R1

First day of the first full calendar year that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirements R2, R3, and R4

First day of the first full calendar year that is 36 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 36 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Planning Coordinator shall, at least once each calendar year, provide notification of each generator, transformer, and transmission line BES Element in its area that meets one or more of the following criteria, if any, to the respective Generator Owner and Transmission Owner: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

Criteria:

1. Generator(s) where an angular stability constraint exists that is addressed by a limiting the output of a generator or a Remedial Action Scheme (RAS), and those Elements terminating at the Transmission station associated with the generator(s).
2. Elements associated with angular instability identified in Planning Assessments.
3. An Element that forms the boundary of an island in the most recent underfrequency load shedding (UFLS) design assessment based on application of the Planning Coordinator's criteria for identifying islands, only if the island is formed by tripping the Element due to angular instability.
4. An Element identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[1] power swing during a simulated disturbance.

M1. Each Planning Coordinator shall have dated evidence that demonstrates notification of the generator, transformer, and transmission line BES Element(s) that meet one or more of the criteria in Requirement R1, if any, to the respective Generator Owner and Transmission Owner. Evidence may include, but is not limited to, the following documentation: emails, facsimiles, records, reports, transmittals, lists, or spreadsheets.

[1] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

R2. Each Generator Owner and Transmission Owner shall: [Violation Risk Factor: High] [Time Horizon: Operations Planning]

2.1 Within 12 full calendar months of notification of a BES Element pursuant to Requirement R1, determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B where an evaluation of that Element's load-responsive protective relay(s) based on PRC-026-1 – Attachment B criteria has not been performed in the last five calendar years.

2.2 Within 12 full calendar months of becoming aware[2] of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable[3] power swing due to the operation of its protective relay(s), determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B.

M2. Each Generator Owner and Transmission Owner shall have dated evidence that demonstrates the evaluation was performed according to Requirement R2. Evidence may include, but is not limited to, the following documentation: apparent impedance characteristic plots, email, design drawings, facsimiles, R-X plots, software output, records, reports, transmittals, lists, settings sheets, or spreadsheets.

R3. Each Generator Owner and Transmission Owner shall, within six full calendar months of determining a load-responsive protective relay does not meet the PRC-026-1 – Attachment B criteria pursuant to Requirement R2, develop a Corrective Action Plan (CAP) to meet one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- The Protection System meets the PRC-026-1 – Attachment B criteria, while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element); or
- The Protection System is excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element).

M3. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates the development of a CAP in accordance with Requirement R3. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

R4. Each Generator Owner and Transmission Owner shall implement each CAP developed pursuant to Requirement R3 and update each CAP if actions or timetables change until all actions are complete. *[Violation Risk Factor: Medium][Time Horizon: Long-Term Planning]*

M4. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates implementation of each CAP according to Requirement R4, including updates to the CAP when actions or timetables change. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

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 Generator Owner, Planning Coordinator, and Transmission Owner 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 Planning Coordinator shall retain evidence of Requirement R1 for a minimum of one calendar year following the completion of the Requirement.
- The Generator Owner and Transmission Owner shall retain evidence of Requirement R2 evaluation for a minimum of 12 calendar months following completion of each evaluation where a CAP is not developed.
- The Generator Owner and Transmission Owner shall retain evidence of Requirements R2, R3, and R4 for a minimum of 12 calendar months following completion of each CAP.

If a Generator Owner, Planning Coordinator, or Transmission Owner 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.

[2] Some examples of the ways an entity may become aware of a power swing are provided in the Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing."

[3] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure; "Compliance Monitoring and Assessment Processes" 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.

Table of Compliance Elements

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was less than or equal to 30 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 90 calendar days late. OR The Planning Coordinator failed to provide notification of the BES Element(s) in accordance with Requirement R1.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	High	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was less than or equal to 30 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 90 calendar days late. OR The Generator Owner or Transmission Owner failed to evaluate its load-responsive protective relay(s) in accordance with Requirement R2.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Long-term Planning	Medium	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than six calendar months and less than or equal to seven calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than seven calendar months and less than or equal to eight calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than eight calendar months and less than or equal to nine calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than nine calendar months. OR The Generator Owner or Transmission Owner failed to develop a CAP in accordance with Requirement R3.
R4	Long-term Planning	Medium	The Generator Owner or Transmission Owner implemented a Corrective Action Plan (CAP), but failed to update a CAP when actions or timetables changed, in accordance with Requirement R4.	N/A	N/A	The Generator Owner or Transmission Owner failed to implement a Corrective Action Plan (CAP) in accordance with Requirement R4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Applied Protective Relaying, Westinghouse Electric Corporation, 1979.

Burdy, John, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

IEEE Power System Relaying Committee WG D6, *Power Swing and Out-of-Step Considerations on Transmission Lines*, July 2005: http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Kimbark Edward Wilson, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

Kundur, Prabha, *Power System Stability and Control*, 1994, Palo Alto: EPRI, McGraw Hill, Inc.

NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf.

Reimert, Donald, *Protective Relaying for Power Generation Systems*, 2006, Boca Raton: CRC Press.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by NERC Board of Trustees	New
1	March 17, 2016	FERC Order issued approving PRC-026-1. Docket No. RM15-8-000.	

PRC-026-1 – Attachment A

This standard applies to any protective functions which could trip instantaneously or with a time delay of less than 15 cycles on load current (i.e., "load-responsive") including, but not limited to:

- Phase distance
- Phase overcurrent
- Out-of-step tripping
- Loss-of-field

The following protection functions are excluded from Requirements of this standard:

- Relay elements supervised by power swing blocking
- Relay elements that are only enabled when other relays or associated systems fail. For example:
    - Overcurrent elements that are only enabled during loss of potential conditions.
    - Relay elements that are only enabled during a loss of communications
- Thermal emulation relays which are used in conjunction with dynamic Facility Ratings
- Relay elements associated with direct current (dc) lines
- Relay elements associated with dc converter transformers
- Phase fault detector relay elements employed to supervise other load-responsive phase distance elements (i.e., in order to prevent false operation in the event of a loss of potential)
- Relay elements associated with switch-onto-fault schemes
- Reverse power relay on the generator
- Generator relay elements that are armed only when the generator is disconnected from the system, (e.g., non-directional overcurrent elements used in conjunction with inadvertent energization schemes, and open breaker flashover schemes)
- Current differential relay, pilot wire relay, and phase comparison relay
- Voltage-restrained or voltage-controlled overcurrent relays

PRC-026-1 – Attachment B

Criterion A:

An impedance-based relay used for tripping is expected to not trip for a stable power swing, when the relay characteristic is completely contained within the unstable power swing region.[4] The unstable power swing region is formed by the union of three shapes in the impedance (R-X) plane; (1) a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7; (2) an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43; (3) a lens that connects the endpoints of the total system impedance (with the parallel transfer impedance removed) bounded by varying the sending-end and receiving-end voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance where:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.

[4] Guidelines and Technical Basis, Figures 1 and 2.

PRC-026-1 – Attachment B

Criterion B:

The pickup of an overcurrent relay element used for tripping, that is above the calculated current value (with the parallel transfer impedance removed) for the conditions below:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.
4. Both the sending-end and receiving-end voltages at 1.05 per unit.

Guidelines and Technical Basis

Introduction

The NERC System Protection and Control Subcommittee technical document, *Protection System Response to Power Swings*, August 2013,[5] ("PSRPS Report" or "report") was specifically prepared to support the development of this NERC Reliability Standard. The report provided a historical perspective on power swings as early as 1965 up through the approval of the report by the NERC Planning Committee. The report also addresses reliability issues regarding trade-offs between security and dependability of Protection Systems, considerations for this NERC Reliability Standard, and a collection of technical information about power swing characteristics and varying issues with practical applications and approaches to power swings. Of these topics, the report suggests an approach for this NERC Reliability Standard ("standard" or "PRC-026-1") which is consistent with addressing three regulatory directives in the FERC Order No. 733. The first directive concerns the need for "…protective relay systems that differentiate between faults and stable power swings and, when necessary, phases out protective relay systems that cannot meet this requirement."[6] Second, is "…to develop a Reliability Standard addressing undesirable relay operation due to stable power swings."[7] The third directive "…to consider "islanding" strategies that achieve the fundamental performance for all islands in developing the new Reliability Standard addressing stable power swings"[8] was considered during development of the standard.

The development of this standard implements the majority of the approaches suggested by the report. However, it is noted that the Reliability Coordinator and Transmission Planner have not been included in the standard's Applicability section (as suggested by the PSRPS Report). This is so that a single entity, the Planning Coordinator, may be the single source for identifying Elements according to Requirement R1. A single source will insure that multiple entities will not identify Elements in duplicate, nor will one entity fail to provide an Element because it believes the Element is being provided by another entity. The Planning Coordinator has, or has access to, the wide-area model and can correctly identify the Elements that may be susceptible to a stable or unstable power swing. Additionally, not including the Reliability Coordinator and Transmission Planner is consistent with the applicability of other relay loadability NERC Reliability Standards (e.g., PRC-023 and PRC-025). It is also consistent with the NERC Functional Model.

The phrase, "while maintaining dependable fault detection and dependable out-of-step tripping" in Requirement R3, describes that the Generator Owner and Transmission Owner are to comply with this standard while achieving its desired protection goals. Load-responsive protective relays, as addressed within this standard, may be intended to provide a variety of backup protection functions, both within the generating unit or generating plant and on the transmission system, and

---

[5] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

[6] Transmission Relay Loadability Reliability Standard, Order No. 733, P.150 FERC ¶ 61,221 (2010).

[7] Ibid. P.153.

[8] Ibid. P.162.

this standard is not intended to result in the loss of these protection functions. Instead, the Generator Owner and Transmission Owner must consider both the Requirements within this standard and its desired protection goals and perform modifications to its protective relays or protection philosophies as necessary to achieve both.

Power Swings

The IEEE Power System Relaying Committee WG D6 developed a technical document called *Power Swing and Out-of-Step Considerations on Transmission Lines* (July 2005) that provides background on power swings. The following are general definitions from that document:[9]

> Power Swing: a variation in three phase power flow which occurs when the generator rotor angles are advancing or retarding relative to each other in response to changes in load magnitude and direction, line switching, loss of generation, faults, and other system disturbances.
>
> Pole Slip: a condition whereby a generator, or group of generators, terminal voltage angles (or phases) go past 180 degrees with respect to the rest of the connected power system.
>
> Stable Power Swing: a power swing is considered stable if the generators do not slip poles and the system reaches a new state of equilibrium, i.e. an acceptable operating condition.
>
> Unstable Power Swing: a power swing that will result in a generator or group of generators experiencing pole slipping for which some corrective action must be taken.
>
> Out-of-Step Condition: Same as an unstable power swing.
>
> Electrical System Center or Voltage Zero: it is the point or points in the system where the voltage becomes zero during an unstable power swing.

Burden to Entities

The PSRPS Report provides a technical basis and approach for focusing on Protection Systems, which are susceptible to power swings, while achieving the purpose of the standard. The approach reduces the number of relays to which the PRC-026-1 Requirements would apply by first identifying the BES Element(s) on which load-responsive protective relays must be evaluated. The first step uses criteria to identify the Elements on which a Protection System is expected to be challenged by power swings. Of those Elements, the second step is to evaluate each load-responsive protective relay that is applied on each identified Element. Rather than requiring the Planning Coordinator or Transmission Planner to perform simulations to obtain information for each identified Element, the Generator Owner and Transmission Owner will reduce the need for simulation by comparing the load-responsive protective relay characteristic to specific criteria in PRC-026-1 – Attachment B.

[9] http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Applicability

The standard is applicable to the Generator Owner, Planning Coordinator, and Transmission Owner entities. More specifically, the Generator Owner and Transmission Owner entities are applicable when applying load-responsive protective relays at the terminals of the applicable BES Elements. The standard is applicable to the following BES Elements: generators, transformers, and transmission lines. The Distribution Provider was considered for inclusion in the standard; however, it is not subject to the standard because this entity, by functional registration, would not own generators, transmission lines, or transformers other than load serving.

Load-responsive protective relays include any protective functions which could trip with or without time delay, on load current.

Requirement R1

The Planning Coordinator has a wide-area view and is in the position to identify what, if any, Elements meet the criteria. The criterion-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document, *Protection System Response to Power Swings (*August 2013),[10] which recommends a focused approach to determine an at-risk Element. Identification of Elements comes from the annual Planning Assessments pursuant to the transmission planning (i.e., "TPL") and other NERC Reliability Standards (e.g., PRC-006), and the standard is not requiring any other assessments to be performed by the Planning Coordinator. The required notification on a calendar year basis to the respective Generator Owner and Transmission Owner is sufficient because it is expected that the Planning Coordinator will make its notifications following the completion of its annual Planning Assessments. The Planning Coordinator will continue to provide notification of Elements on a calendar year basis even if a study is performed less frequently (e.g., PRC-006 – Automatic Underfrequency Load Shedding, which is five years) and has not changed. It is possible that a Planning Coordinator could utilize studies from a prior year in determining the necessary notifications pursuant to Requirement R1.

Criterion 1

The first criterion involves generator(s) where an angular stability constraint exists that is addressed by limiting the output of a generator or a Remedial Action Scheme (RAS) and those Elements terminating at the Transmission station associated with the generator(s). For example, a scheme to remove generation for specific conditions is implemented for a four-unit generating plant (1,100 MW). Two of the units are 500 MW each; one is connected to the 345 kV system and one is connected to the 230 kV system. The Transmission Owner has two 230 kV transmission lines and one 345 kV transmission line all terminating at the generating facility as well as a 345/230 kV autotransformer. The remaining 100 MW consists of two 50 MW combustion turbine (CT) units connected to four 66 kV transmission lines. The 66 kV transmission lines are not electrically joined to the 345 kV and 230 kV transmission lines at the plant site and are not subject to any generating output limitation or RAS. A stability constraint limits the output of the portion of the

[10] http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

plant affected by the RAS to 700 MW for an outage of the 345 kV transmission line. The RAS trips one of the 500 MW units to maintain stability for a loss of the 345 kV transmission line when the total output from both 500 MW units is above 700 MW. For this example, both 500 MW generating units and the associated generator step-up (GSU) transformers would be identified as Elements meeting this criterion. The 345/230 kV autotransformer, the 345 kV transmission line, and the two 230 kV transmission lines would also be identified as Elements meeting this criterion. The 50 MW combustion turbines and 66 kV transmission lines would not be identified pursuant to Criterion 1 because these Elements are not subject to any generating output limitation or RAS and do not terminate at the Transmission station associated with the generators that are subject to any generating output limitation or RAS.

Criterion 2

The second criterion involves Elements associated with angular instability identified in the Planning Assessments. For example, if Planning Assessments have identified that an angular instability could limit transfer capability on two long parallel 500 kV transmission lines to a maximum of 1,200 MW, and this limitation is based on angular instability resulting from a fault and subsequent loss of one of the two lines, then both lines would be identified as Elements meeting the criterion.

Criterion 3

The third criterion involves Elements that form the boundary of an island within an underfrequency load shedding (UFLS) design assessment. The criterion applies to islands identified based on application of the Planning Coordinator's criteria for identifying islands, where the island is formed by tripping the Elements based on angular instability. The criterion applies if the angular instability is modeled in the UFLS design assessment, or if the boundary is identified "off-line" (i.e., the Elements are selected based on angular instability considerations, but the Elements are tripped in the UFLS design assessment without modeling the initiating angular instability). In cases where an out-of-step condition is detected and tripping is initiated at an alternate location, the criterion applies to the Element on which the power swing is detected. The criterion does not apply to islands identified based on other considerations that do not involve angular instability, such as excessive loading, Planning Coordinator area boundary tie lines, or Balancing Authority boundary tie lines.

Criterion 4

The fourth criterion involves Elements identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[11] power swing during a simulated disturbance. The intent is for the Planning Coordinator to include any Element(s) where relay tripping was observed during simulations performed for the most recent annual Planning Assessment associated with the transmission planning TPL-001-4 Reliability Standard. Note that

[11] Refer to the "Justification for Including Unstable Power Swings in the Requirements" section.

relay tripping must be assessed within those annual Planning Assessments per TPL-001-4, R4, Part 4.3.1.3, which indicates that analysis shall include the "Tripping of Transmission lines and transformers where transient swings cause Protection System operation based on generic or actual relay models." Identifying such Elements according to Criterion 4 and notifying the respective Generator Owner and Transmission Owner will require that the owners of any load-responsive protective relay applied at the terminals of the identified Element evaluate the relay's susceptibility to tripping in response to a stable power swing.

Planning Coordinators have the discretion to determine whether the observed tripping for a power swing in its Planning Assessments occurs for valid contingencies and system conditions. The Planning Coordinator will address tripping that is observed in transient analyses on an individual basis; therefore, the Planning Coordinator is responsible for identifying the Elements based only on simulation results that are determined to be valid.

Due to the nature of how a Planning Assessment is performed, there may be cases where a previously-identified Element is not identified in the most recent annual Planning Assessment. If so, this is acceptable because the Generator Owner and Transmission Owner would have taken action upon the initial notification of the previously identified Element. When an Element is not identified in later Planning Assessments, the risk of load-responsive protective relays tripping in response to a stable power swing during non-Fault conditions would have already been assessed under Requirement R2 and mitigated according to Requirements R3 and R4 where the relays did not meet the PRC-026-1 – Attachment B criteria. According to Requirement R2, the Generator Owner and Transmission Owner are only required to re-evaluate each load-responsive protective relay for an identified Element where the evaluation has not been performed in the last five calendar years.

Although Requirement R1 requires the Planning Coordinator to notify the respective Generator Owner and Transmission Owner of any Elements meeting one or more of the four criteria, it does not preclude the Planning Coordinator from providing additional information, such as apparent impedance characteristics, in advance or upon request, that may be useful in evaluating protective relays. Generator Owners and Transmission Owners are able to complete protective relay evaluations and perform the required actions without additional information. The standard does not include any requirement for the entities to provide information that is already being shared or exchanged between entities for operating needs. While a Requirement has not been included for the exchange of information, entities should recognize that relay performance needs to be measured against the most current information.

Requirement R2

Requirement R2 requires the Generator Owner and Transmission Owner to evaluate its load-responsive protective relays to ensure that they are expected to not trip in response to stable power swings.

The PRC-026-1 – Attachment A lists the applicable load-responsive relays that must be evaluated which include phase distance, phase overcurrent, out-of-step tripping, and loss-of-field relay functions. Phase distance relays could include, but are not limited to, the following:

- Zone elements with instantaneous tripping or intentional time delays of less than 15 cycles
- Phase distance elements used in high-speed communication-aided tripping schemes including:
  - Directional Comparison Blocking (DCB) schemes
  - Directional Comparison Un-Blocking (DCUB) schemes
  - Permissive Overreach Transfer Trip (POTT) schemes
  - Permissive Underreach Transfer Trip (PUTT) schemes

A method is provided within the standard to support consistent evaluation by Generator Owners and Transmission Owners based on specified conditions. Once a Generator Owner or Transmission Owner is notified of Elements pursuant to Requirement R1, it has 12 full calendar months to determine if each Element's load-responsive protective relays meet the PRC-026-1 – Attachment B criteria, if the determination has not been performed in the last five calendar years. Additionally, each Generator Owner and Transmission Owner, that becomes aware of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable power swing due to the operation of its protective relays pursuant to Requirement R2, Part 2.2, must perform the same PRC-026-1 – Attachment B criteria determination within 12 full calendar months.

Becoming Aware of an Element That Tripped in Response to a Power Swing

Part 2.2 in Requirement R2 is intended to initiate action by the Generator Owner and Transmission Owner when there is a known stable or unstable power swing and it resulted in the entity's Element tripping. The criterion starts with becoming aware of the event (i.e., power swing) and then any connection with the entity's Element tripping. By doing so, the focus is removed from the entity having to demonstrate that it made a determination whether a power swing was present for every Element trip. The basis for structuring the criterion in this manner is driven by the available ways that a Generator Owner and Transmission Owner could become aware of an Element that tripped in response to a stable or unstable power swing due to the operation of its protective relay(s).

Element trips caused by stable or unstable power swings, though infrequent, would be more common in a larger event. The identification of power swings will be revealed during an analysis of the event. Event analysis where an entity may become aware of a stable or unstable power swing could include internal analysis conducted by the entity, the entity's Protection System review following a trip, or a larger scale analysis by other entities. Event analysis could include involvement by the entity's Regional Entity, and in some cases NERC.

Information Common to Both Generation and Transmission Elements

The PRC-026-1 – Attachment A lists the load-responsive protective relays that are subject to this standard. Generator Owners and Transmission Owners may own load-responsive protective relays (e.g., distance relays) that directly affect generation or transmission BES Elements and will require analysis as a result of Elements being identified by the Planning Coordinator in Requirement R1

or the Generator Owner or Transmission Owner in Requirement R2. For example, distance relays owned by the Transmission Owner may be installed at the high-voltage side of the generator step-up (GSU) transformer (directional toward the generator) providing backup to generation protection. Generator Owners may have distance relays applied to backup transmission protection or backup protection to the GSU transformer. The Generator Owner may have relays installed at the generator terminals or the high-voltage side of the GSU transformer.

Exclusion of Time Based Load-Responsive Protective Relays

The purpose of the standard is "[t]o ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions." Load-responsive, high-speed tripping protective relays pose the highest risk of operating during a power swing. Because of this, high-speed tripping protective relays and relays with a time delay of less than 15 cycles are included in the standard; whereas other relays (i.e., Zones 2 and 3) with a time delay of 15 cycles or greater are excluded. The time delay used for exclusion on some load-responsive protective relays is based on the maximum expected time that load-responsive protective relays would be exposed to a stable power swing with a slow slip rate frequency.

In order to establish a time delay that distinguishes a high-risk load-responsive protective relay from one that has a time delay for tripping (lower-risk), a sample of swing rates were calculated based on a stable power swing entering and leaving the impedance characteristic as shown in Table 1. For a relay impedance characteristic that has a power swing entering and leaving, beginning at 90 degrees with a termination at 120 degrees before exiting the zone, the zone timer must be greater than the calculated time the stable power swing is inside the relay's operating zone to not trip in response to the stable power swing.

Eq. (1) $$Zone\ timer > 2 \times \left(\frac{(120° - Angle\ of\ entry\ into\ the\ relay\ characteristic) \times 60}{(360 \times Slip\ Rate)}\right)$$

Table 1: Swing Rates

Zone Timer (Cycles)	Slip Rate (Hz)
10	1.00
15	0.67
20	0.50
30	0.33

With a minimum zone timer of 15 cycles, the corresponding slip rate of the system is 0.67 Hz. This represents an approximation of a slow slip rate during a system Disturbance. Longer time delays allow for slower slip rates.

Application to Transmission Elements

Criterion A in PRC-026-1 – Attachment B describes an unstable power swing region that is formed by the union of three shapes in the impedance (R-X) plane. The first shape is a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7 (i.e., E_S / E_R = 0.7 / 1.0 = 0.7). The second shape is an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43 (i.e., E_S / E_R = 1.0 / 0.7 = 1.43). The third shape is a lens that connects the endpoints of the total system impedance together by varying the sending-end and receiving-end system voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance (with the parallel transfer impedance removed—see Figures 1 through 5). The total system impedance is derived from a two-bus equivalent network and is determined by summing the sending-end source impedance, the line impedance (excluding the Thévenin equivalent transfer impedance), and the receiving-end source impedance as shown in Figures 6 and 7. Establishing the total system impedance provides a conservative condition that will maximize the security of the relay against various system conditions. The smallest total system impedance represents a condition where the size of the lens characteristic in the R-X plane is smallest and is a conservative operating point from the standpoint of ensuring a load-responsive protective relay is expected to not trip given a predetermined angular displacement between the sending-end and receiving-end voltages. The smallest total system impedance results when all generation is in service and all transmission BES Elements are modeled in their "normal" system configuration (PRC-026-1 – Attachment B, Criterion A). The parallel transfer impedance is removed to represent a likely condition where parallel Elements may be lost during the disturbance, and the loss of these Elements magnifies the sensitivity of the load-responsive relays on the parallel line by removing the "infeed effect" (i.e., the apparent impedance sensed by the relay is decreased as a result of the loss of the transfer impedance, thus making the relay more likely to trip for a stable power swing—See Figures 13 and 14).

The sending-end and receiving-end source voltages are varied from 0.7 to 1.0 per unit to form the lower and upper loss-of-synchronism circles. The ratio of these two voltages is used in the calculation of the loss-of-synchronism circles, and result in a ratio range from 0.7 to 1.43.

Eq. (2) $$\frac{E_S}{E_R} = \frac{0.7}{1.0} = 0.7$$

Eq. (3): $$\frac{E_S}{E_R} = \frac{1.0}{0.7} = 1.43$$

The internal generator voltage during severe power swings or transmission system fault conditions will be greater than zero due to voltage regulator support. The voltage ratio of 0.7 to 1.43 is chosen to be more conservative than the PRC-023[12] and PRC-025[13] NERC Reliability Standards where a lower bound voltage of 0.85 per unit voltage is used. A ±15% internal generator voltage range was chosen as a conservative voltage range for calculation of the voltage ratio used to calculate the loss-of-synchronism circles. For example, the voltage ratio using these voltages would result in a ratio range from 0.739 to 1.353.

[12] Transmission Relay Loadability

[13] Generator Relay Loadability

Eq. (4) $$\frac{E_S}{E_R} = \frac{0.85}{1.15} = 0.739$$ Eq. (5): $$\frac{E_S}{E_R} = \frac{1.15}{0.85} = 1.353$$

The lower ratio is rounded down to 0.7 to be more conservative, allowing a voltage range of 0.7 to 1.0 per unit to be used for the calculation of the loss-of-synchronism circles.[14]

When the parallel transfer impedance is included in the model, the division of current through the parallel transfer impedance path results in actual measured relay impedances that are larger than those measured when the parallel transfer impedance is removed (i.e., infeed effect), which would make it more likely for an impedance relay element to be completely contained within the unstable power swing region as shown in Figure 11. If the transfer impedance is included in the evaluation, a distance relay element could be deemed as meeting PRC-026-1 – Attachment B criteria and, in fact would be secure, assuming all Elements were in their normal state. In this case, the distance relay element could trip in response to a stable power swing during an actual event if the system was weakened (i.e., a higher transfer impedance) by the loss of a subset of lines that make up the parallel transfer impedance as shown in Figure 10. This could happen because the subset of lines that make up the parallel transfer impedance tripped on unstable swings, contained the initiating fault, and/or were lost due to operation of breaker failure or remote back-up protection schemes.

Table 10 shows the percent size increase of the lens shape as seen by the relay under evaluation when the parallel transfer impedance is included. The parallel transfer impedance has minimal effect on the apparent size of the lens shape as long as the parallel transfer impedance is at least 10 multiples of the parallel line impedance (less than 5% lens shape expansion), therefore, its removal has minimal impact, but results in a slightly more conservative, smaller lens shape. Parallel transfer impedances of 5 multiples of the parallel line impedance or less result in an apparent lens shape size of 10% or greater as seen by the relay. If two parallel lines and a parallel transfer impedance tie the sending-end and receiving-end buses together, the total parallel transfer impedance will be one or less multiples of the parallel line impedance, resulting in an apparent lens shape size of 45% or greater. It is a realistic contingency that the parallel line could be out-of-service, leaving the parallel transfer impedance making up the rest of the system in parallel with the line impedance. Since it is not known exactly which lines making up the parallel transfer impedance will be out of service during a major system disturbance, it is most conservative to assume that all of them are out, leaving just the line under evaluation in service.

Either the saturated transient or sub-transient direct axis reactance may be used for machines in the evaluation because they are smaller than the un-saturated reactances. Since saturated sub-transient generator reactances are smaller than the transient or synchronous reactances, the use of sub-transient reactances will result in a smaller source impedance and a smaller unstable power swing region in the graphical analysis as shown in Figures 8 and 9. Because power swings occur in a time frame where generator transient reactances will be prevalent, it is acceptable to use saturated transient reactances instead of saturated sub-transient reactances. Because some short-

[14] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, Section 6 (The Cascade Stage of the Blackout), p. 94 under "Why the Generators Tripped Off," states, "Some generator undervoltage relays were set to trip at or above 90% voltage. However, a motor stalls out at about 70% voltage and a motor starter contactor drops out around 75%, so if there is a compelling need to protect the turbine from the system the under-voltage trigger point should be no higher than 80%."

circuit models may not include transient reactances, the use of sub-transient reactances is also acceptable because it produces more conservative results. For this reason, either value is acceptable when determining the system source impedances (PRC-026-1 – Attachment B, Criterion A and B, No. 3).

Saturated reactances are used in short-circuit programs that produce the system impedance mentioned above. Planning and stability software generally use un-saturated reactances. Generator models used in transient stability analyses recognize that the extent of the saturation effect depends upon both rotor (field) and stator currents. Accordingly, they derive the effective saturated parameters of the machine at each instant by internal calculation from the specified (constant) unsaturated values of machine reactances and the instantaneous internal flux level. The specific assumptions regarding which inductances are affected by saturation, and the relative effect of that saturation, are different for the various generator models used. Thus, unsaturated values of all machine reactances are used in setting up planning and stability software data, and the appropriate set of open-circuit magnetization curve data is provided for each machine.

Saturated reactance values are smaller than unsaturated reactance values and are used in short-circuit programs owned by the Generator and Transmission Owners. Because of this, saturated reactance values are to be used in the development of the system source impedances.

The source or system equivalent impedances can be obtained by a number of different methods using commercially available short-circuit calculation tools.[15] Most short-circuit tools have a network reduction feature that allows the user to select the local and remote terminal buses to retain. The first method reduces the system to one that contains two buses, an equivalent generator at each bus (representing the source impedances at the sending-end and receiving-end), and two parallel lines; one being the line impedance of the protected line with relays being analyzed, the other being the parallel transfer impedance representing all other combinations of lines that connect the two buses together as shown in Figure 6. Another conservative method is to open both ends of the line being evaluated, and apply a three-phase bolted fault at each bus to determine the Thévenin equivalent impedance at each bus. The source impedances are set equal to the Thévenin equivalent impedances and will be less than or equal to the actual source impedances calculated by the network reduction method. Either method can be used to develop the system source impedances at both ends.

The two bullets of PRC-026-1 – Attachment B, Criterion A, No. 1, identify the system separation angles used to identify the size of the power swing stability boundary for evaluating load-responsive protective relay impedance elements. The first bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates a system separation angle of at least 120 degrees that is held constant while varying the sending-end and receiving-end source voltages from 0.7 to 1.0 per unit, thus creating an unstable power swing region about the total system impedance in Figure 1. This unstable power swing region is compared to the tripping portion of the distance relay characteristic; that is, the portion that is not supervised by load encroachment, blinders, or some other form of supervision as shown in Figure 12 that restricts the distance element from tripping

[15] Demetrios A. Tziouvaras and Daqing Hou, Appendix in *Out-Of-Step Protection Fundamentals and Advancements,* April 17, 2014: https://www.selinc.com.

for heavy, balanced load conditions. If the tripping portion of the impedance characteristics are completely contained within the unstable power swing region, the relay impedance element meets Criterion A in PRC-026-1 – Attachment B. A system separation angle of 120 degrees was chosen for the evaluation because it is generally accepted in the industry that recovery for a swing beyond this angle is unlikely to occur.[16]

The second bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates impedance relay elements at a system separation angle of less than 120 degrees, similar to the first bullet described above. An angle less than 120 degrees may be used if a documented stability analysis demonstrates that the power swing becomes unstable at a system separation angle of less than 120 degrees.

The exclusion of relay elements supervised by Power Swing Blocking (PSB) in PRC-026-1 – Attachment A allows the Generator Owner or Transmission Owner to exclude protective relay elements if they are blocked from tripping by PSB relays. A PSB relay applied and set according to industry accepted practices prevent supervised load-responsive protective relays from tripping in response to power swings. Further, PSB relays are set to allow dependable tripping of supervised elements. The criteria in PRC-026-1 – Attachment B specifically applies to unsupervised elements that could trip for stable power swings. Therefore, load-responsive protective relay elements supervised by PSB can be excluded from the Requirements of this standard.

[16] "The critical angle for maintaining stability will vary depending on the contingency and the system condition at the time the contingency occurs; however, the likelihood of recovering from a swing that exceeds 120 degrees is marginal and 120 degrees is generally accepted as an appropriate basis for setting out-of-step protection. Given the importance of separating unstable systems, defining 120 degrees as the critical angle is appropriate to achieve a proper balance between dependable tripping for unstable power swings and secure operation for stable power swings." NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf), p. 28.

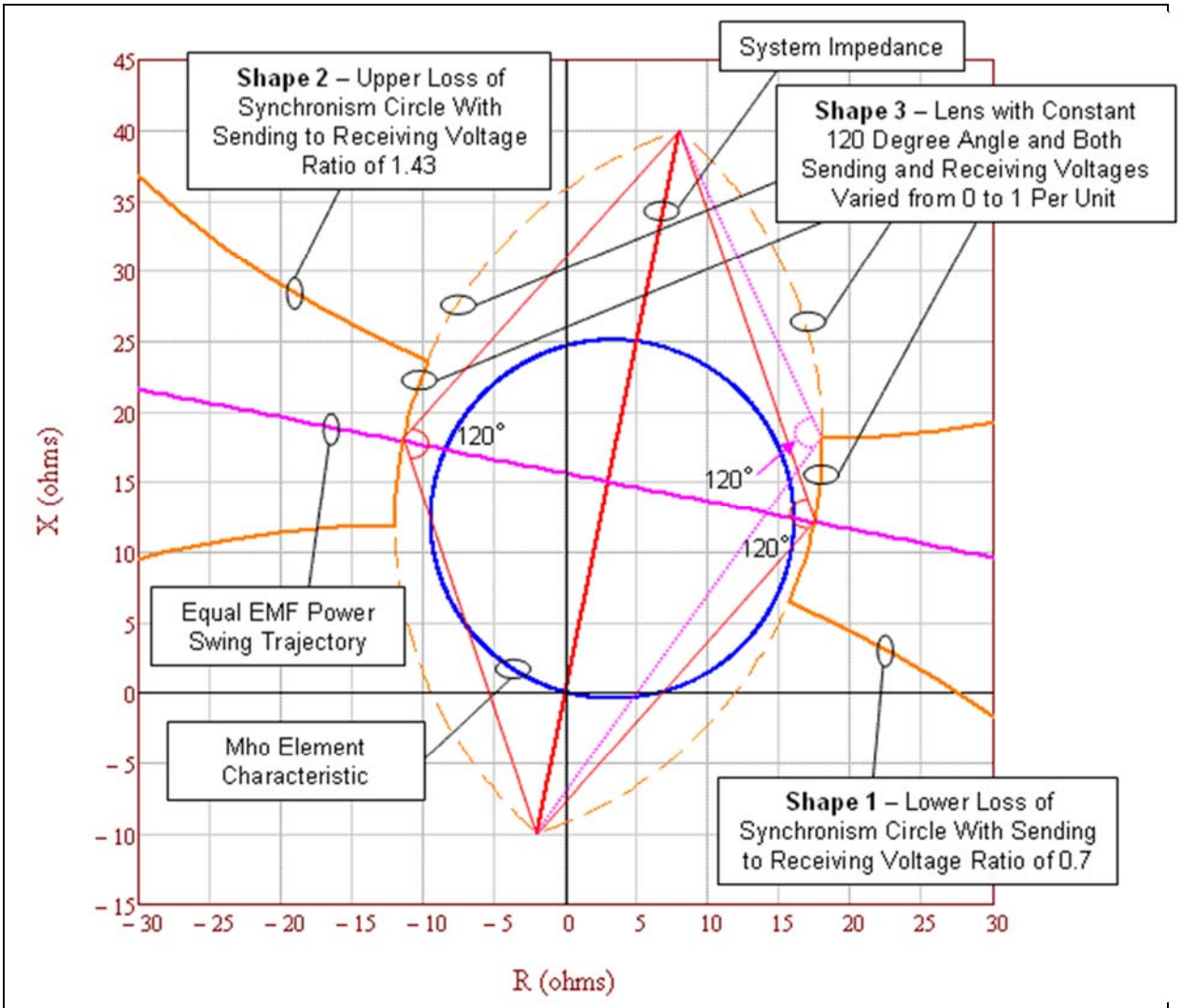


Figure 1: An enlarged graphic illustrating the unstable power swing region formed by the union of three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region (i.e., it does not intersect any portion of the unstable power swing region), therefore it meets PRC-026-1 – Attachment B, Criterion A, No. 1.

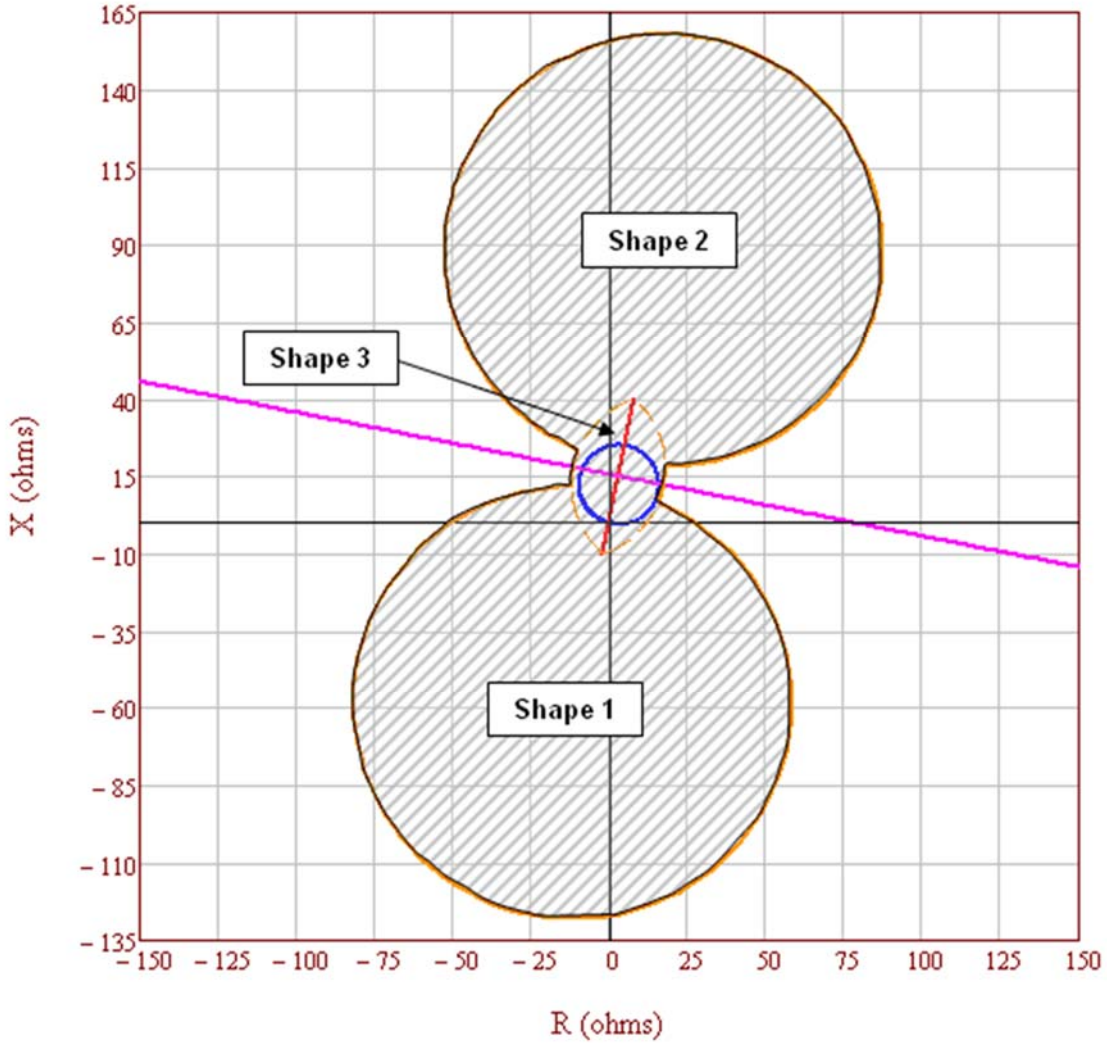


Figure 2: Full graphic of the unstable power swing region formed by the union of the three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region, therefore it meets PRC-26-1 – Attachment B, Criterion A, No.1.

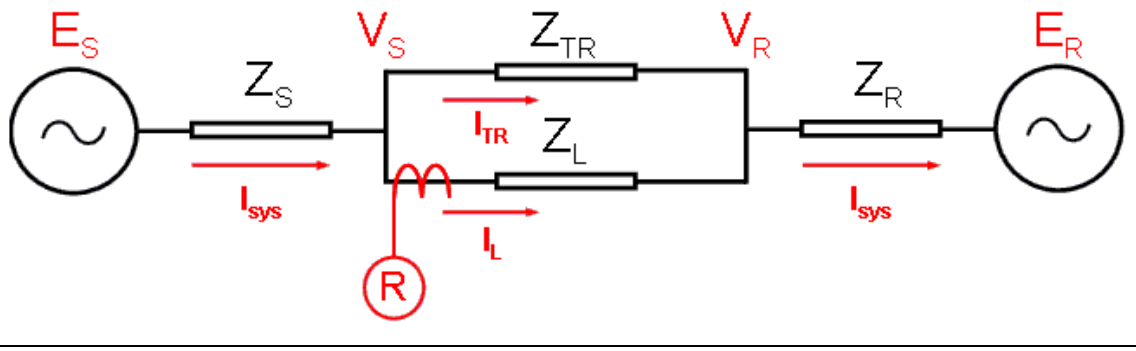


Figure 3: System impedances as seen by Relay R (voltage connections are not shown).

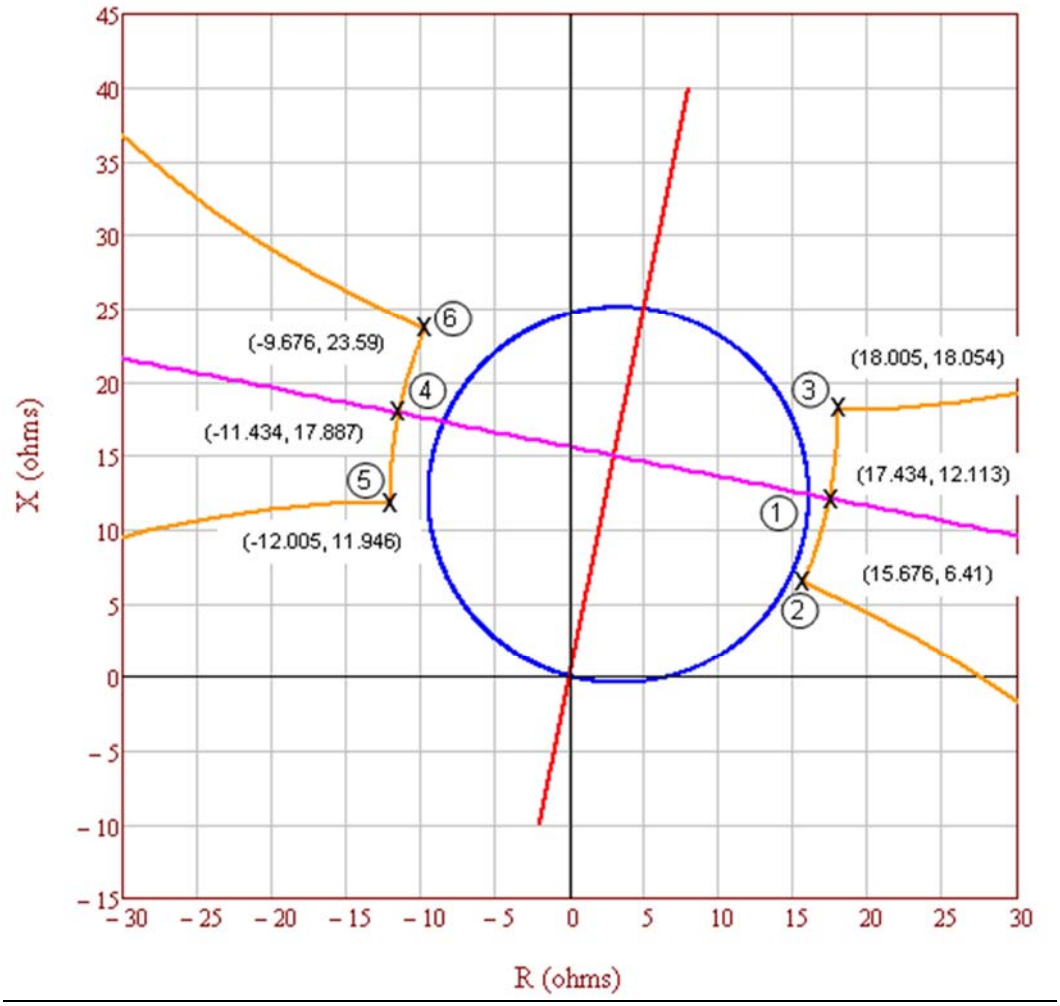


Figure 4: The defining unstable power swing region points where the lens shape intersects the lower and upper loss-of-synchronism circle shapes and where the lens intersects the equal EMF (electromotive force) power swing.

E_S / E_R Voltage Ratio	Left Side Coordinates R	Left Side Coordinates + jX	Right Side Coordinates R	Right Side Coordinates + jX
0.7	**-12.005**	**11.946**	**15.676**	**6.41**
0.72	-12.004	12.407	15.852	6.836
0.74	-11.996	12.857	16.018	7.255
0.76	-11.982	13.298	16.175	7.667
0.78	-11.961	13.729	16.321	8.073
0.8	-11.935	14.151	16.459	8.472
0.82	-11.903	14.563	16.589	8.865
0.84	-11.867	14.966	16.71	9.251
0.86	-11.826	15.361	16.824	9.631
0.88	-11.78	15.746	16.93	10.004
0.9	-11.731	16.123	17.03	10.371
0.92	-11.678	16.492	17.123	10.732
0.94	-11.621	16.852	17.209	11.086
0.96	-11.562	17.205	17.29	11.435
0.98	-11.499	17.55	17.364	11.777
1	**-11.434**	**17.887**	**17.434**	**12.113**
1.0286	-11.336	18.356	17.524	12.584
1.0572	-11.234	18.81	17.604	13.043
1.0858	-11.127	19.251	17.675	13.49
1.1144	-11.017	19.677	17.738	13.926
1.143	-10.904	20.091	17.792	14.351
1.1716	-10.788	20.491	17.84	14.766
1.2002	-10.67	20.88	17.88	15.17
1.2288	-10.55	21.256	17.914	15.564
1.2574	-10.428	21.621	17.942	15.948
1.286	-10.304	21.975	17.964	16.322
1.3146	-10.18	22.319	17.981	16.687
1.3432	-10.054	22.652	17.993	17.043
1.3718	-9.928	22.976	18.001	17.39
1.4004	-9.801	23.29	18.005	17.728
1.429	**-9.676**	**23.59**	**18.005**	**18.054**

Figure 5: Full table of 31 detailed lens shape point calculations. The bold highlighted rows correspond to the detailed calculations in Tables 2-7.

Table 2: Example Calculation (Lens Point 1)	
This example is for calculating the impedance the first point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 120 degrees. See Figures 3 and 4.	
Eq. (6)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$

Table 2: Example Calculation (Lens Point 1)			
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (7)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (8)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (9)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (10)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50\ )\Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (11)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		

Table 2: Example Calculation (Lens Point 1)	
	$I_L = 4{,}511\angle 71.3° \; A \times \frac{(4 + j20) \times 10^{10} \; \Omega}{(4 + j20) \; \Omega + (4 + j20) \times 10^{10} \; \Omega}$
	$I_L = 4{,}511\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (12)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10) \; \Omega \times 4{,}511\angle 71.3° \; A]$
	$V_S = 95{,}757\angle 106.1° \; V$
The impedance seen by the relay on Z_L.	
Eq. (13)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \; V}{4{,}511\angle 71.3° \; A}$
	$Z_{L-Relay} = 17.434 + j12.113 \; \Omega$

Table 3: Example Calculation (Lens Point 2)			
This example is for calculating the impedance second point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (14)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 120° \; V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 120° \; V$		
Eq. (15)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \; V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \; V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10 \; \Omega$	$Z_L = 4 + j20 \; \Omega$	$Z_R = 4 + j20 \; \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10} \; \Omega$		

Table 3: Example Calculation (Lens Point 2)	
Total impedance between the generators.	
Eq. (16)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (17)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (18)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50)\ \Omega}$
	$I_{sys} = 3{,}854\angle 77°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (19)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 77°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 77°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (20)	$V_S = E_S - \left(Z_S \times I_{sys}\right)$
	$V_S = 92{,}953\angle 120°\ V - [(2 + j10\ )\Omega \times 3{,}854\angle 77°\ A]$
	$V_S = 65{,}271\angle 99°\ V$
The impedance seen by the relay on Z_L.	
Eq. (21)	$Z_{L-Relay} = \frac{V_S}{I_L}$

Table 3: Example Calculation (Lens Point 2)	
	$Z_{L-Relay} = \frac{65{,}271\angle 99° \, V}{3{,}854\angle 77° \, A}$
	$Z_{L-Relay} = 15.676 + j6.41 \, \Omega$

Table 4: Example Calculation (Lens Point 3)			
This example is for calculating the impedance third point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (22)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120° \, V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120° \, V$		
Eq. (23)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0° \, V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0° \, V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10 \, \Omega$	$Z_L = 4 + j20 \, \Omega$	$Z_R = 4 + j20 \, \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10} \, \Omega$		
Total impedance between the generators.			
Eq. (24)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20) \, \Omega \times (4 + j20) \times 10^{10} \, \Omega\right)}{\left((4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega\right)}$		
	$Z_{total} = 4 + j20 \, \Omega$		
Total system impedance.			
Eq. (25)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10) \, \Omega + (4 + j20) \, \Omega + (4 + j20) \, \Omega$		
	$Z_{sys} = 10 + j50 \, \Omega$		

Table 4: Example Calculation (Lens Point 3)	
Total system current from sending-end source.	
Eq. (26)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{132{,}791\angle 120° \, V - 92{,}953.7\angle 0° \, V}{(10 + j50) \, \Omega}$
	$I_{sys} = 3{,}854\angle 65.5° \, A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (27)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 65.5° \, A \times \frac{(4 + j20) \times 10^{10} \, \Omega}{(4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega}$
	$I_L = 3{,}854\angle 65.5° \, A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (28)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 120° \, V - [(2 + j10) \, \Omega \times 3{,}854\angle 65.5° \, A]$
	$V_S = 98{,}265\angle 110.6° \, V$
The impedance seen by the relay on Z_L.	
Eq. (29)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle 110.6° \, V}{3{,}854\angle 65.5° \, A}$
	$Z_{L-Relay} = 18.005 + j18.054 \, \Omega$

Table 5: Example Calculation (Lens Point 4)	
This example is for calculating the impedance fourth point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 240 degrees. See Figures 3 and 4.	
Eq. (30)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 240° \, V}{\sqrt{3}}$

Table 5: Example Calculation (Lens Point 4)			
	$E_S = 132{,}791\angle 240° \, V$		
Eq. (31)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \, V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \, V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10 \, \Omega$	$Z_L = 4 + j20 \, \Omega$	$Z_R = 4 + j20 \, \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10} \, \Omega$		
Total impedance between the generators.			
Eq. (32)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20) \, \Omega \times (4 + j20) \times 10^{10} \, \Omega\right)}{\left((4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega\right)}$		
	$Z_{total} = 4 + j20 \, \Omega$		
Total system impedance.			
Eq. (33)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10) \, \Omega + (4 + j20) \, \Omega + (4 + j20) \, \Omega$		
	$Z_{sys} = 10 + j50 \, \Omega$		
Total system current from sending-end source.			
Eq. (34)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240° \, V - 132{,}791\angle 0° \, V}{(10 + j50 \,)\Omega}$		
	$I_{sys} = 4{,}511\angle 131.3° \, A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (35)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 131.1° \, A \times \frac{(4 + j20) \times 10^{10} \, \Omega}{(4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega}$		
	$I_L = 4{,}511\angle 131.1° \, A$		

Table 5: Example Calculation (Lens Point 4)			
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.			
Eq. (36)	$V_S = E_S - (Z_S \times I_L)$		
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10\,)\,\Omega \times 4{,}511\angle 131.1° \, A]$		
	$V_S = 95{,}756\angle -106.1° \, V$		
The impedance seen by the relay on Z_L.			
Eq. (37)	$Z_{L-Relay} = \frac{V_S}{I_L}$		
	$Z_{L-Relay} = \frac{95{,}756\angle -106.1° \, V}{4{,}511\angle 131.1° \, A}$		
	$Z_{L-Relay} = -11.434 + j17.887\ \Omega$		

Table 6: Example Calculation (Lens Point 5)			
This example is for calculating the impedance fifth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (38)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 240° \, V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 240° \, V$		
Eq. (39)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \, V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \, V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (40)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		

Table 6: Example Calculation (Lens Point 5)	
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (41)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10\ \Omega) + (4 + j20\ \Omega) + (4 + j20\ \Omega)$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (42)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 240°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$
	$I_{sys} = 3{,}854\angle 125.5°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (43)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 125.5°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 125.5°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (44)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 92{,}953.7\angle 240°\ V - [(2 + j10\ )\ \Omega \times 3{,}854\angle 125.5°\ A]$
	$V_S = 65{,}270.5\angle -99.4°\ V$
The impedance seen by the relay on Z_L.	
Eq. (45)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{65{,}270.5\angle -99.4°\ V}{3{,}854\angle 125.5°\ A}$
	$Z_{L-Relay} = -12.005 + j11.946\ \Omega$

Table 7: Example Calculation (Lens Point 6)			
This example is for calculating the impedance sixth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (46)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 240°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 240°\ V$		
Eq. (47)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (48)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (49)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (50)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240°\ V - 92{,}953.7\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 3{,}854\angle 137.1°\ A$		

Table 7: Example Calculation (Lens Point 6)	
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (51)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 137.1° \, A \times \frac{(4 + j20) \times 10^{10} \, \Omega}{(4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega}$
	$I_L = 3{,}854\angle 137.1° \, A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (52)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10 \,) \, \Omega \times 3{,}854\angle 137.1° \, A]$
	$V_S = 98{,}265\angle -110.6° \, V$
The impedance seen by the relay on Z_L.	
Eq. (53)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle -110.6° \, V}{3{,}854\angle 137.1° \, A}$
	$Z_{L-Relay} = -9.676 + j23.59 \, \Omega$

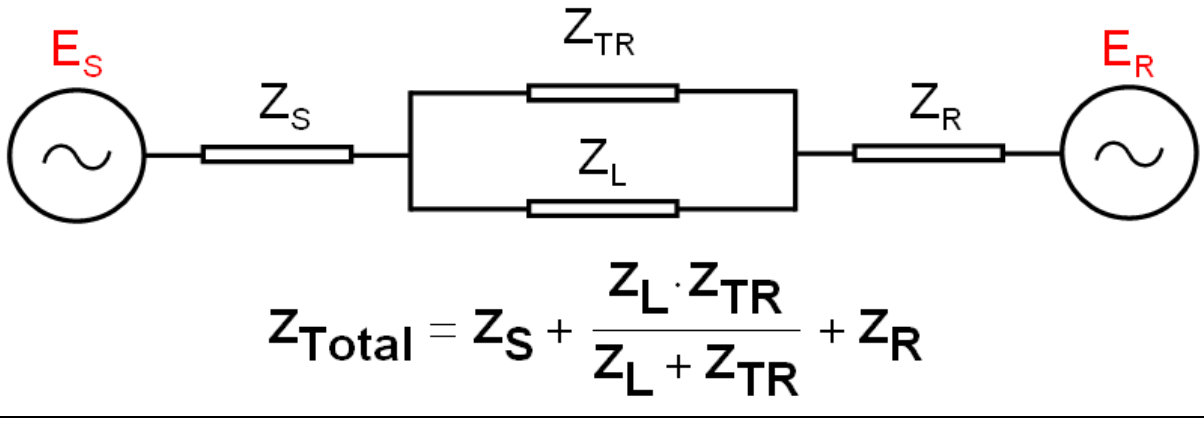


Figure 6: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, line impedance Z_L, and parallel transfer impedance Z_{TR}.

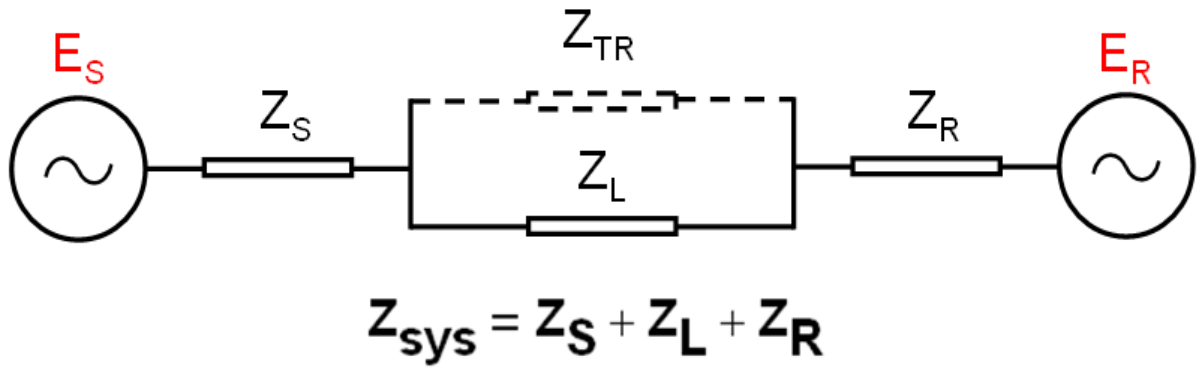


Figure 7: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, and line impedance Z_L with the parallel transfer impedance Z_{TR} removed.

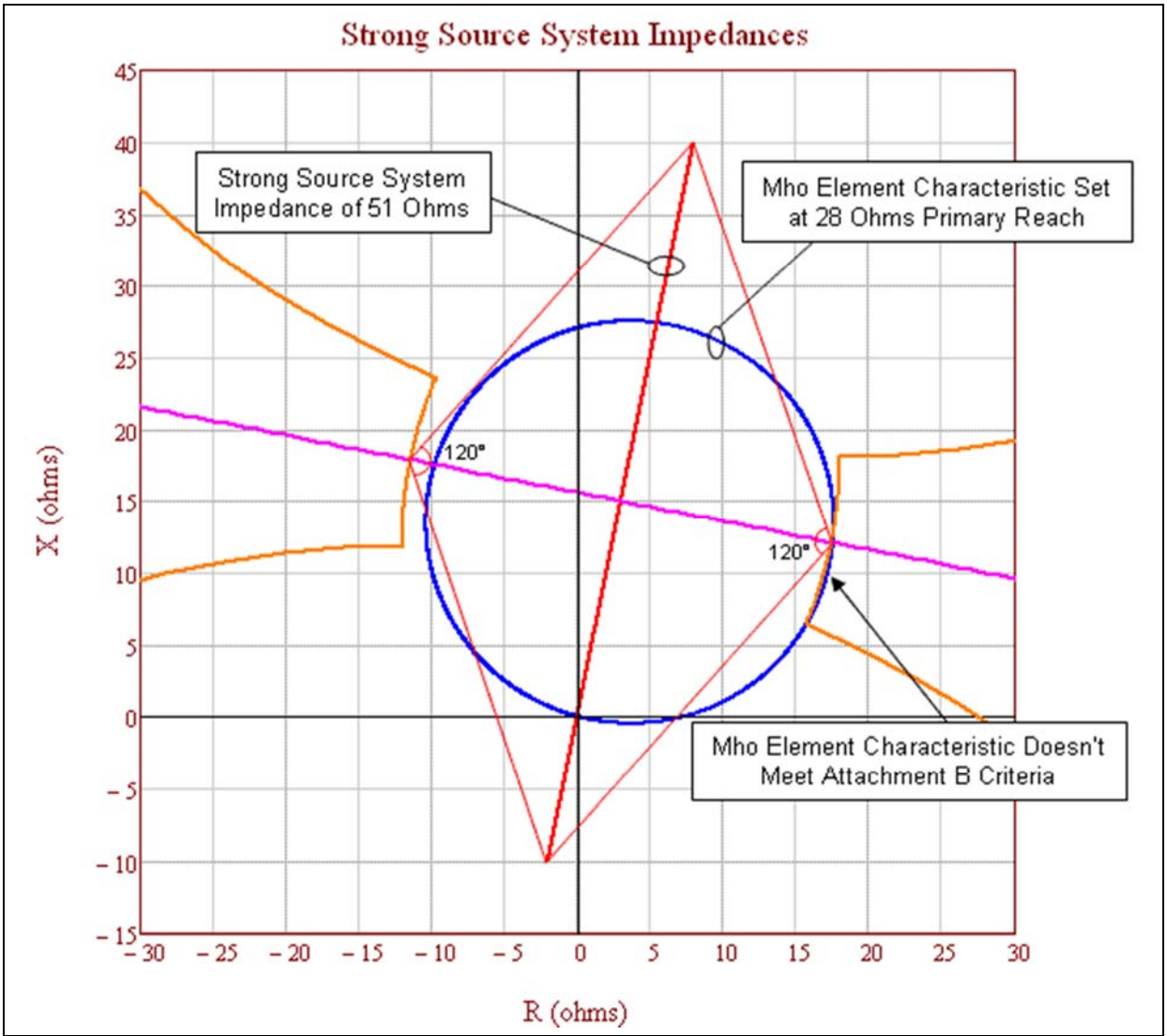


Figure 8: A strong-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) does not meet the PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 8 above represents a heavily-loaded system with all generation in service and all transmission BES Elements in their normal operating state. The mho element characteristic (set at 137% of Z_L) extends into the unstable power swing region (i.e., the orange characteristic). Using the strongest source system is more conservative because it shrinks the unstable power swing region, bringing it closer to the mho element characteristic. This figure also graphically represents the effect of a system strengthening over time and this is the reason for re-evaluation if the relay has not been evaluated in the last five calendar years. Figure 9 below depicts a relay that meets the PRC-026-1 – Attachment B, Criterion A. Figure 8 depicts the same relay with the same setting five years later, where each source has strengthened by about 10% and now the same mho element characteristic does not meet Criterion A.

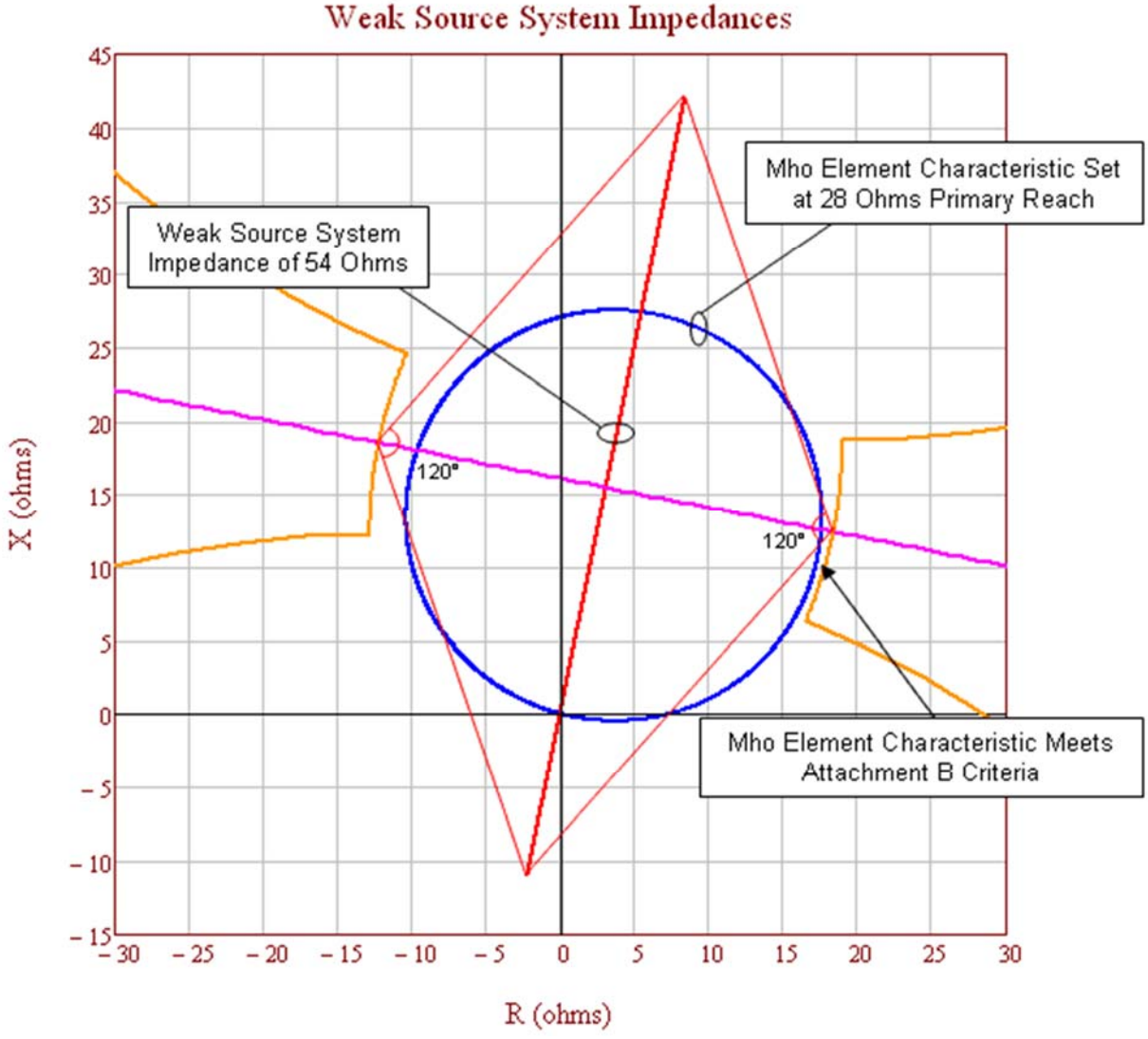


Figure 9: A weak-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) meets the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 9 above represents a lightly-loaded system, using a minimum generation profile. The mho element characteristic (set at 137% of Z_L) does not extend into the unstable power swing region (i.e., the orange characteristic). Using a weaker source system expands the unstable power swing region away from the mho element characteristic.

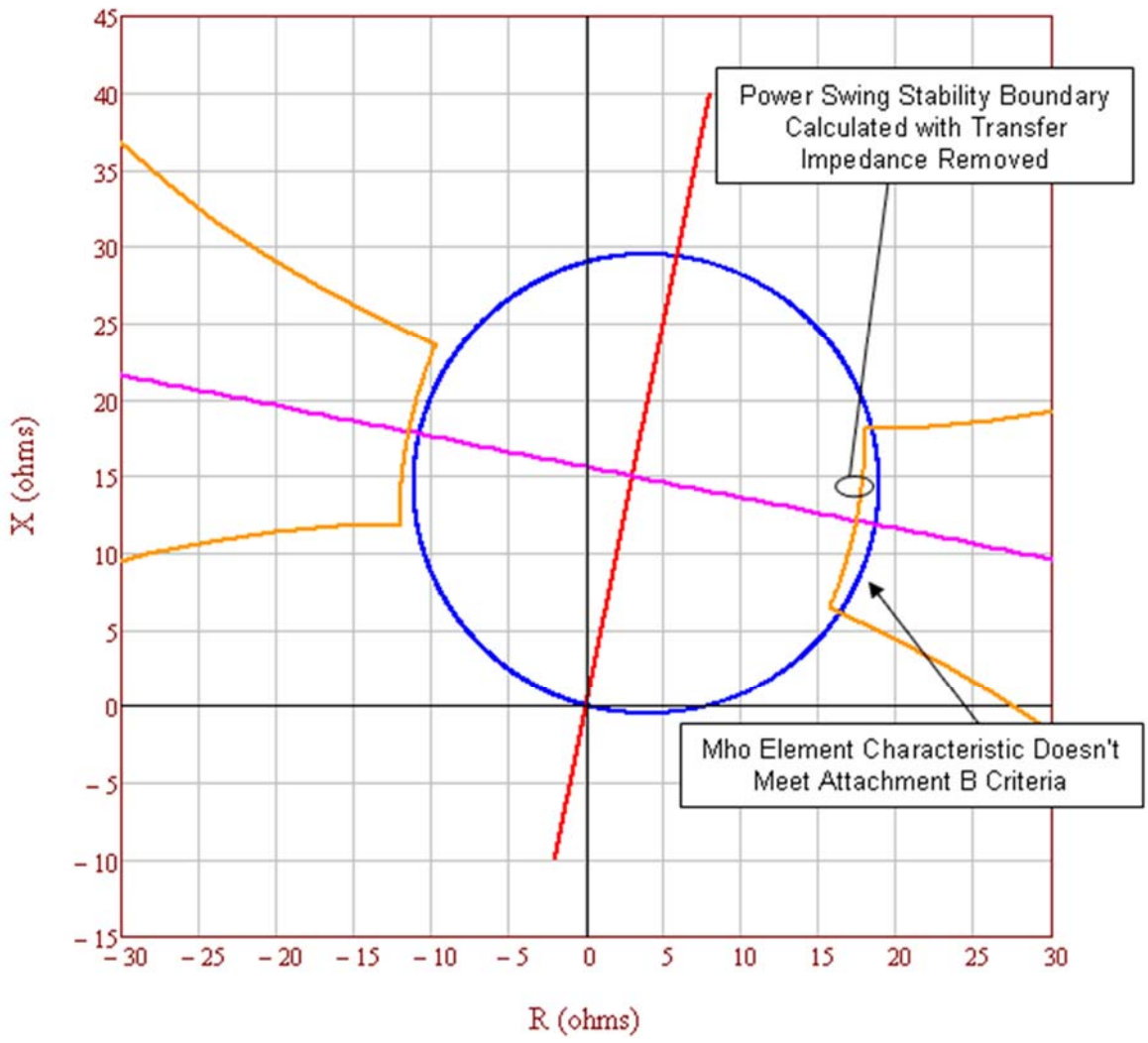


Figure 10: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance removed. This relay mho element characteristic (i.e., the blue circle) does not meet PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region.

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
Calculations for the point at 120 degrees with equal source impedances. The total system current equals the line current. See Figure 10.	
Eq. (54)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$
	$E_S = 132{,}791\angle 120°\ V$

Table 8: Example Calculation (Parallel Transfer Impedance Removed)			
Eq. (55)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (56)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (57)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (58)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (59)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 71.3°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$		
	$I_L = 4{,}511\angle 71.3°\ A$		

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (60)	$V_S = E_S - \left(Z_S \times I_{sys}\right)$
	$V_S = 132{,}791\angle 120° \, V - [(2 + j10\ \Omega) \times 4{,}511\angle 71.3° \, A]$
	$V_S = 95{,}757\angle 106.1° \, V$
The impedance seen by the relay on Z_L.	
Eq. (61)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \, V}{4{,}511\angle 71.3° \, A}$
	$Z_{L-Relay} = 17.434 + j12.113\ \Omega$

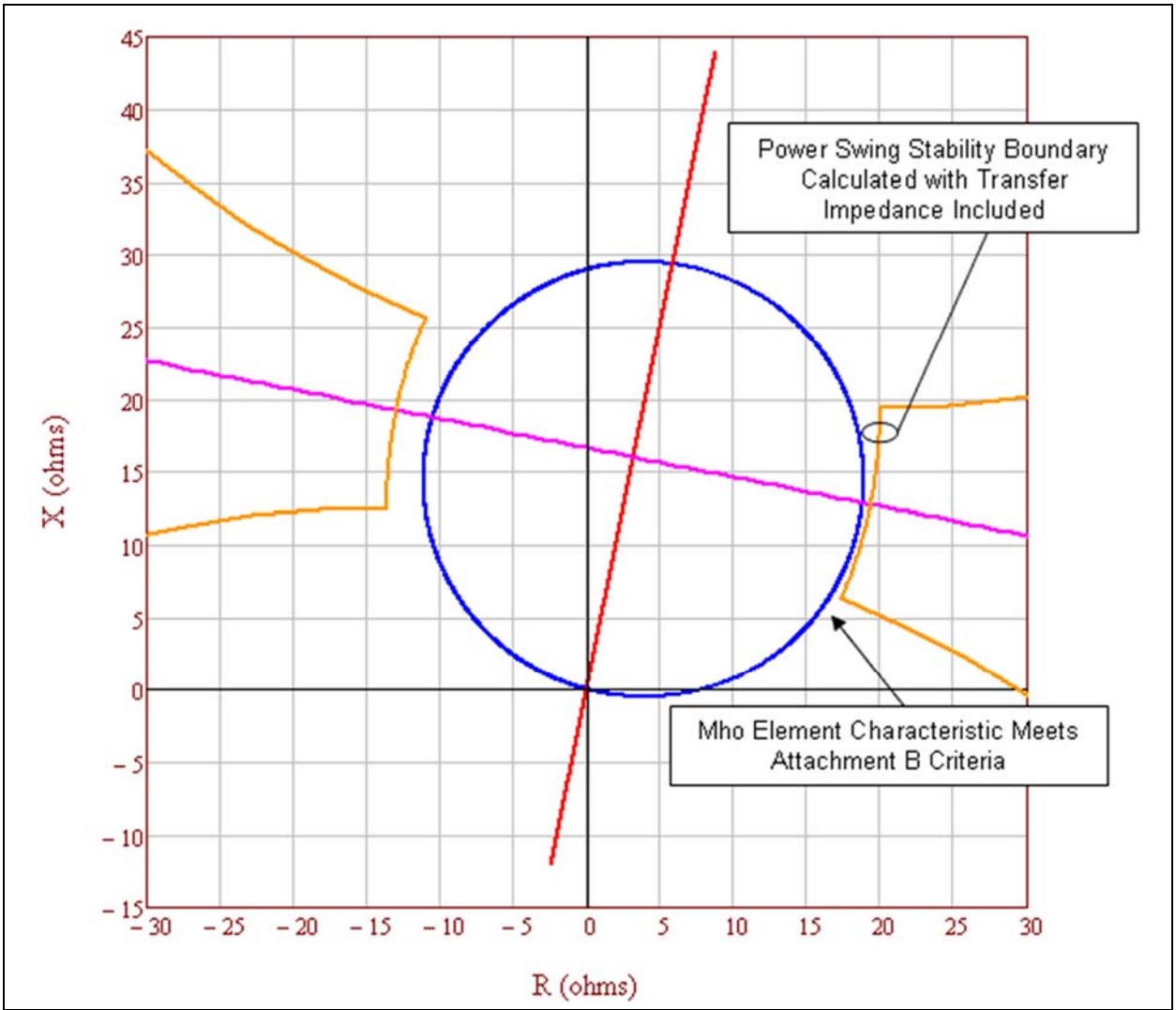


Figure 11: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance included causing the mho element characteristic (i.e., the blue circle) to appear to meet the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

In Figure 11 above, the parallel transfer impedance is 5 times the line impedance. The unstable power swing region has expanded out beyond the mho element characteristic due to the infeed effect from the parallel current through the parallel transfer impedance, thus allowing the mho element characteristic to appear to meet the PRC-026-1 – Attachment B, Criterion A. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

Table 9: Example Calculation (Parallel Transfer Impedance Included)			
Calculations for the point at 120 degrees with equal source impedances. The total system current does not equal the line current. See Figure 11.			
Eq. (62)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (63)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 5$		
	$Z_{TR} = (4 + j20)\ \Omega \times 5$		
	$Z_{TR} = 20 + j100\ \Omega$		
Total impedance between the generators.			
Eq. (64)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{(4 + j20)\ \Omega \times (20 + j100)\ \Omega}{(4 + j20)\ \Omega + (20 + j100)\ \Omega}$		
	$Z_{total} = 3.333 + j16.667\ \Omega$		
Total system impedance.			
Eq. (65)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (3.333 + j16.667)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 9.333 + j46.667\ \Omega$		
Total system current from sending-end source.			
Eq. (66)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{9.333 + j46.667\ \Omega}$		

Table 9: Example Calculation (Parallel Transfer Impedance Included)	
	$I_{sys} = 4{,}833\angle 71.3° \; A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (67)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 4{,}833\angle 71.3° \; A \times \frac{(20 + j100)\;\Omega}{(4 + j20)\;\Omega + (20 + j100)\;\Omega}$
	$I_L = 4{,}027.4\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (68)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10\;\Omega) \times 4{,}833\angle 71.3° \; A]$
	$V_S = 93{,}417\angle 104.7° \; V$
The impedance seen by the relay on Z_L.	
Eq. (69)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{93{,}417\angle 104.7° \; V}{4{,}027\angle 71.3° \; A}$
	$Z_{L-Relay} = 19.366 + j12.767\;\Omega$

Table 10: Percent Increase of a Lens Due To Parallel Transfer Impedance.	
The following demonstrates the percent size increase of the lens characteristic for Z_{TR} in multiples of Z_L with the parallel transfer impedance included.	
Z_{TR} in multiples of Z_L	Percent increase of lens with equal EMF sources (Infinite source as reference)
Infinite	N/A
1000	0.05%
100	0.46%
10	4.63%
5	9.27%
2	23.26%
1	46.76%
0.5	94.14%
0.25	189.56%

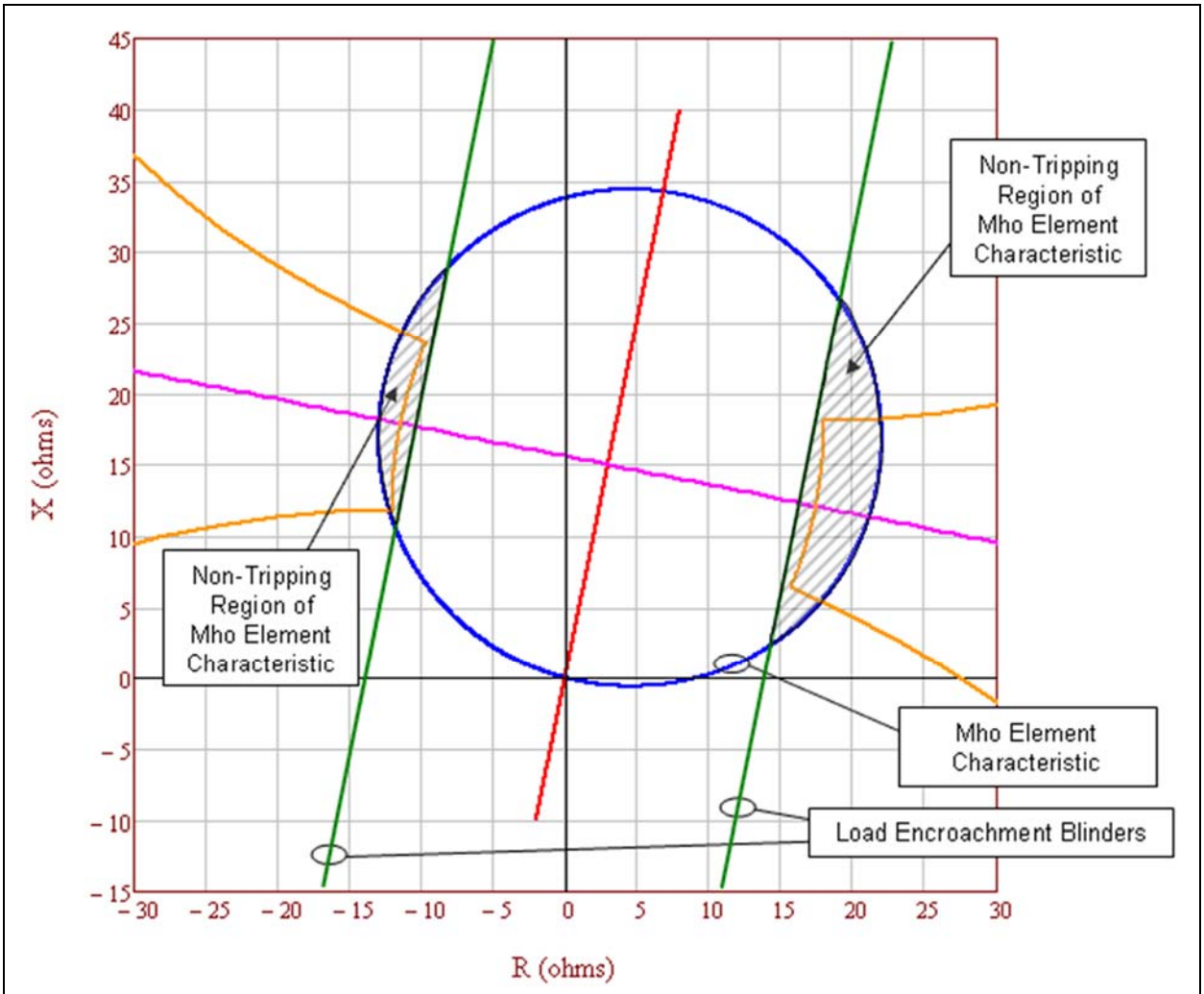


Figure 12: The tripping portion of the mho element characteristic (i.e., the blue circle) not blocked by load encroachment (i.e., the parallel green lines) is completely contained within the unstable power swing region (i.e., the orange characteristic). Therefore, the mho element characteristic meets the PRC-026-1 – Attachment B, Criterion A.

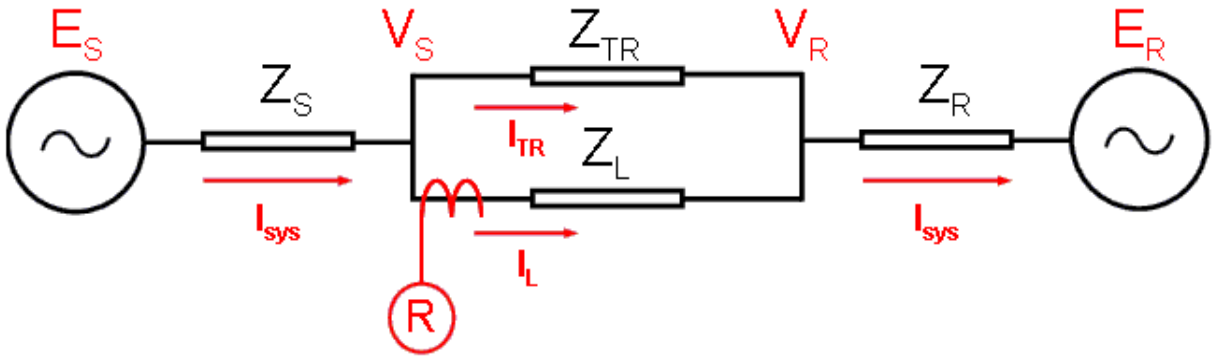


Figure 13: The infeed diagram shows the impedance in front of the relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.

Table 11: Calculations (System Apparent Impedance in the forward direction)

The following equations are provided for calculating the apparent impedance back to the E_R source voltage as seen by relay R. Infeed equations from V_S to source E_R where $E_R = 0$. See Figure 13.

Eq. (70)	$I_L = \frac{V_S - V_R}{Z_L}$			
Eq. (71)	$I_{sys} = \frac{V_R - E_R}{Z_R}$			
Eq. (72)	$I_{sys} = I_L + I_{TR}$			
Eq. (73)	$I_{sys} = \frac{V_R}{Z_R}$	Since $E_R = 0$	Rearranged:	$V_R = I_{sys} \times Z_R$
Eq. (74)	$I_L = \frac{V_S - I_{sys} \times Z_R}{Z_L}$			
Eq. (75)	$I_L = \frac{V_S - [(I_L + I_{TR}) \times Z_R]}{Z_L}$			
Eq. (76)	$V_S = (I_L \times Z_L) + (I_L \times Z_R) + (I_{TR} \times Z_R)$			
Eq. (77)	$Z_{Relay} = \frac{V_S}{I_L} = Z_L + Z_R + \frac{I_{TR} \times Z_R}{I_L} = Z_L + Z_R \times \left(1 + \frac{I_{TR}}{I_L}\right)$			
Eq. (78)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$			
Eq. (79)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$			

Table 11: Calculations (System Apparent Impedance in the forward direction)	
Eq. (80)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$
The infeed equations shows the impedance in front of the relay R (Figure 13) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.	
Eq. (81)	$Z_{Relay} = Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$

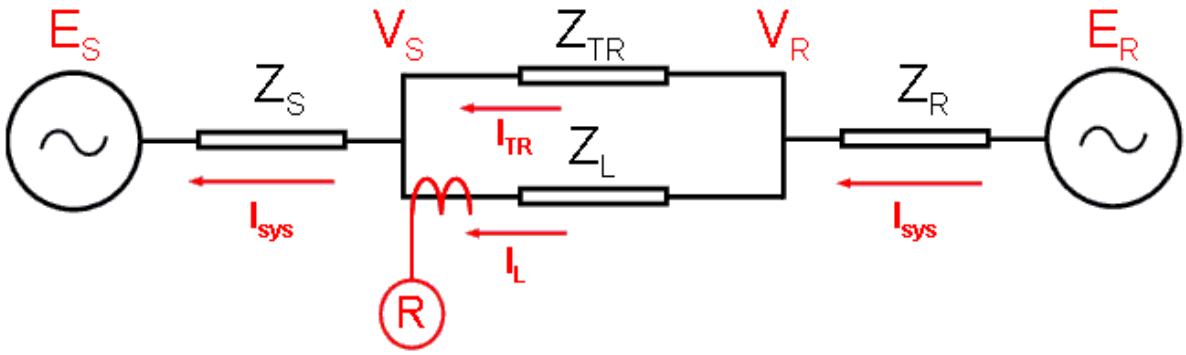


Figure 14: The infeed diagram shows the impedance behind relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)				
The following equations are provided for calculating the apparent impedance back to the E_S source voltage as seen by relay R. Infeed equations from V_R back to source E_S where $E_S = 0$. See Figure 14.				
Eq. (82)	$I_L = \frac{V_R - V_S}{Z_L}$			
Eq. (83)	$I_{sys} = \frac{V_S - E_S}{Z_S}$			
Eq. (84)	$I_{sys} = I_L + I_{TR}$			
Eq. (85)	$I_{sys} = \frac{V_S}{Z_S}$	Since $E_s = 0$	Rearranged:	$V_S = I_{sys} \times Z_S$
Eq. (86)	$I_L = \frac{V_R - I_{sys} \times Z_S}{Z_L}$			

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)		
Eq. (87)	$I_L = \frac{V_R - [(I_L + I_{TR}) \times Z_S]}{Z_L}$	
Eq. (88)	$V_R = (I_L \times Z_L) + (I_L \times Z_S) + (I_{TR} \times Z_{RS})$	
Eq. (89)	$Z_{Relay} = \frac{V_R}{I_L} = Z_L + Z_S + \frac{I_{TR} \times Z_S}{I_L} = Z_L + Z_S \times \left(1 + \frac{I_{TR}}{I_L}\right)$	
Eq. (90)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$	
Eq. (91)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$	
Eq. (92)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$	
The infeed equations shows the impedance behind relay R (Figure 14) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.		
Eq. (93)	$Z_{Relay} = Z_L + Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	As seen by relay R at the receiving-end of the line.
Eq. (94)	$Z_{Relay} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	Subtract Z_L for relay R impedance as seen at sending-end of the line.

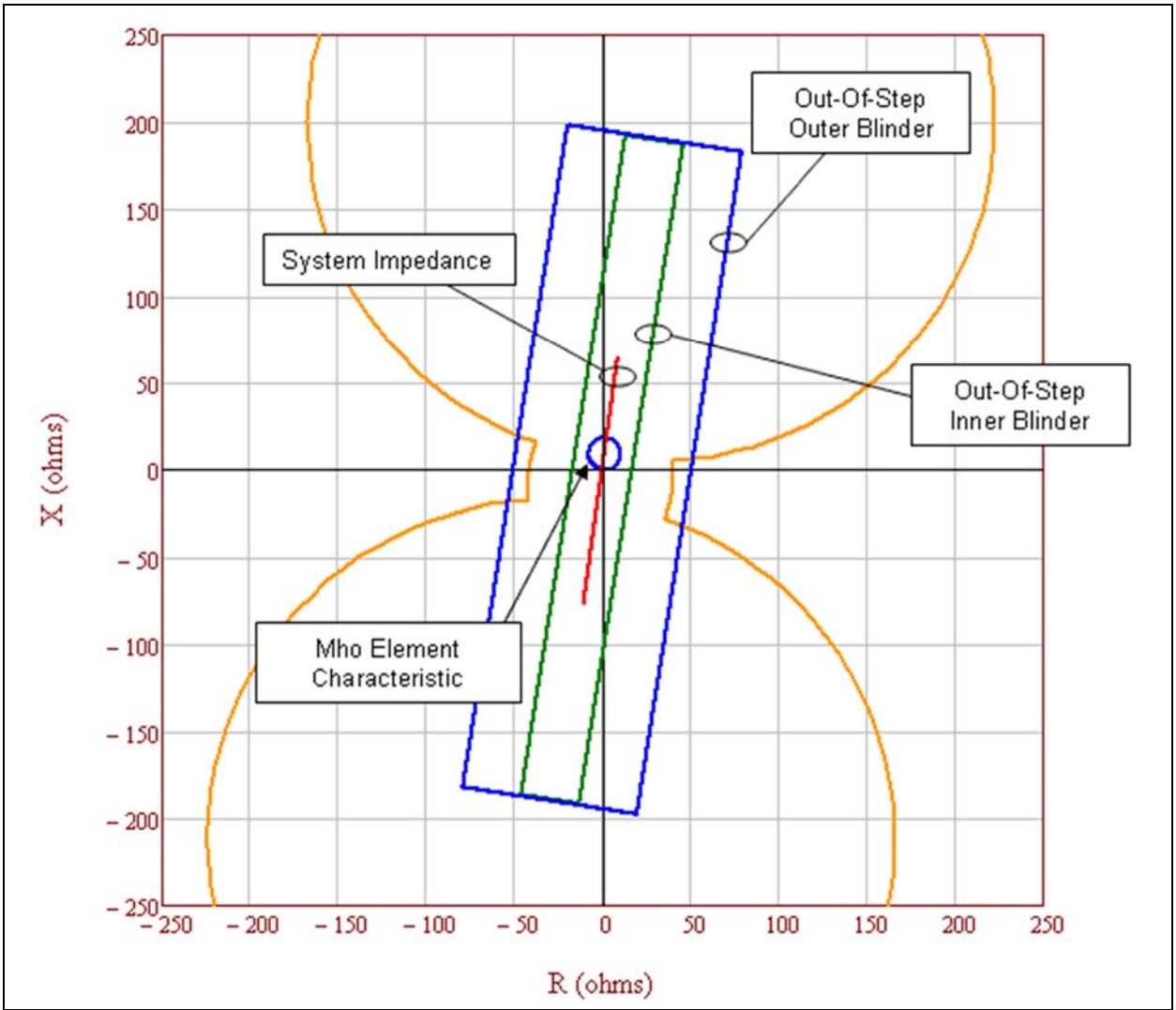


Figure 15: Out-of-step trip (OST) inner blinder (i.e., the parallel green lines) meets the PRC-026-1 – Attachment B, Criterion A because the inner OST blinder initiates tripping either On-The-Way-In or On-The-Way-Out. Since the inner blinder is completely contained within the unstable power swing region (i.e., the orange characteristic), it meets the PRC-026-1 – Attachment B, Criterion A.

Table 13: Example Calculation (Voltage Ratios)			
These calculations are based on the loss-of-synchronism characteristics for the cases of N < 1 and N > 1 as found in the *Application of Out-of-Step Blocking and Tripping Relays*, GER-3180, p. 12, Figure 3.[17] The GE illustration shows the formulae used to calculate the radius and center of the circles that make up the ends of the portion of the lens.			
Voltage ratio equations, source impedance equation with infeed formulae applied, and circle equations.			
Given:	$E_S = 0.7$	$E_R = 1.0$	
Eq. (95)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{0.7}{1.0} = 0.7$		
The total system impedance as seen by the relay with infeed formulae applied.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
	$Z_{TR} = (4 + j20) \times 10^{10}\ \Omega$		
Eq. (96)	$Z_{sys} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right) + \left[Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right]$		
	$Z_{sys} = 10 + j50\ \Omega$		
The calculated coordinates of the lower loss-of-synchronism circle center.			
Eq. (97)	$Z_{C1} = -\left[Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right] - \left[\frac{N^2 \times Z_{sys}}{1 - N^2}\right]$		
	$Z_{C1} = -\left[(2 + j10)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega}\right)\right] - \left[\frac{0.7^2 \times (10 + j50)\ \Omega}{1 - 0.7^2}\right]$		
	$Z_{C1} = -11.608 - j58.039\ \Omega$		
The calculated radius of the lower loss-of-synchronism circle.			
Eq. (98)	$r_a = \left\lvert \frac{N \times Z_{sys}}{1 - N^2} \right\rvert$		
	$r_a = \left\lvert \frac{0.7 \times (10 + j50)\ \Omega}{1 - 0.7^2} \right\rvert$		
	$r_a = 69.987\ \Omega$		
The calculated coordinates of the upper loss-of-synchronism circle center.			
Given:	$E_S = 1.0$	$E_R = 0.7$	

[17] http://store.gedigitalenergy.com/faq/Documents/Alps/GER-3180.pdf

Table 13: Example Calculation (Voltage Ratios)	
Eq. (99)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{1.0}{0.7} = 1.43$
Eq. (100)	$Z_{C2} = Z_L + \left[Z_R \times \left(1 + \frac{Z_L}{Z_{TR}} \right) \right] + \left[\frac{Z_{sys}}{N^2 - 1} \right]$
	$Z_{C2} = 4 + j20\ \Omega + \left[(4 + j20)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega} \right) \right] + \left[\frac{(10 + j50)\ \Omega}{1.43^2 - 1} \right]$
	$Z_{C2} = 17.608 + j88.039\ \Omega$
The calculated radius of the upper loss-of-synchronism circle.	
Eq. (101)	$r_b = \left\lvert \frac{N \times Z_{sys}}{N^2 - 1} \right\rvert$
	$r_b = \left\lvert \frac{1.43 \times (10 + j50)\ \Omega}{1.43^2 - 1} \right\rvert$
	$r_b = 69.987\ \Omega$

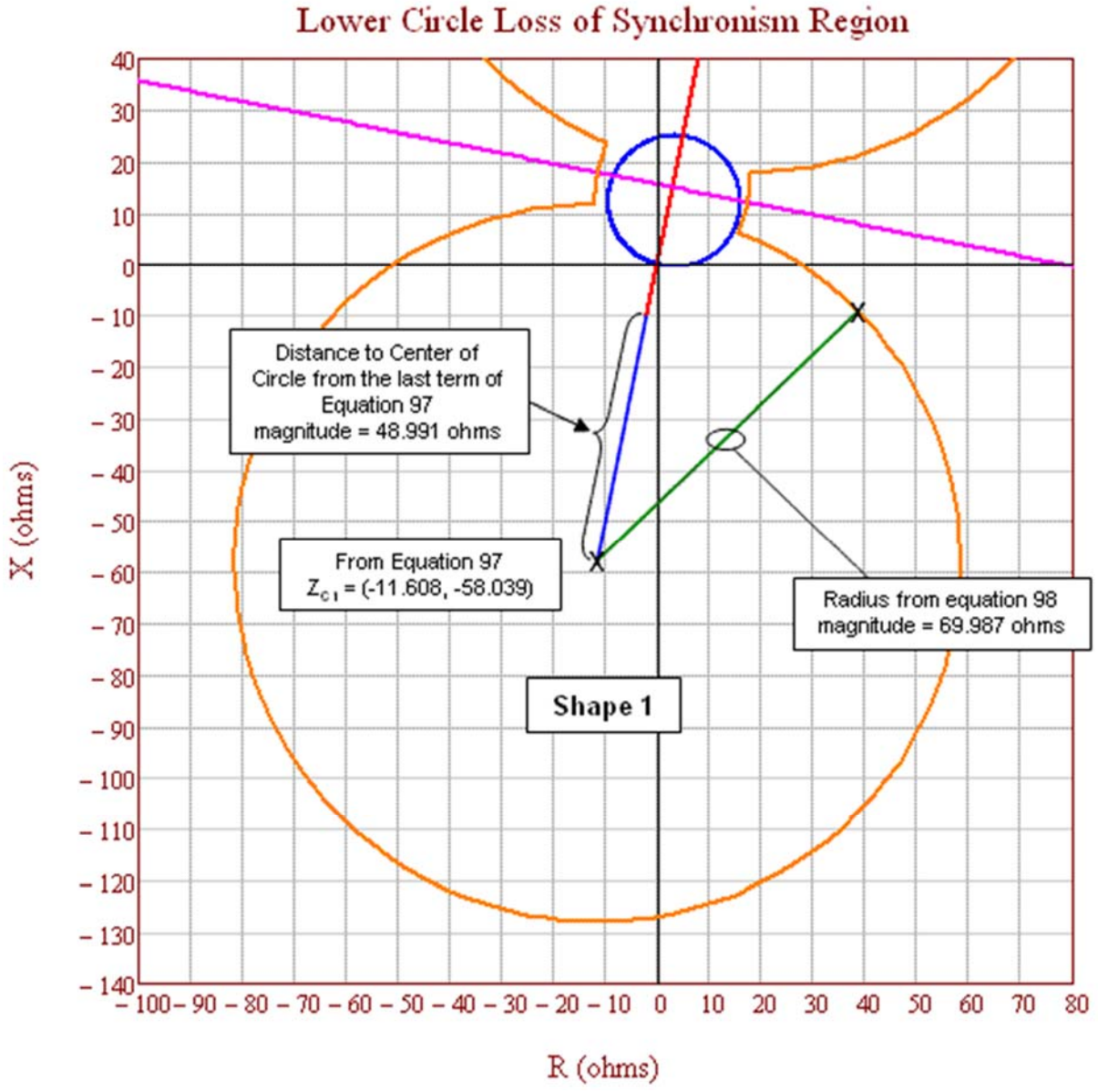


Figure 15a: Lower circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

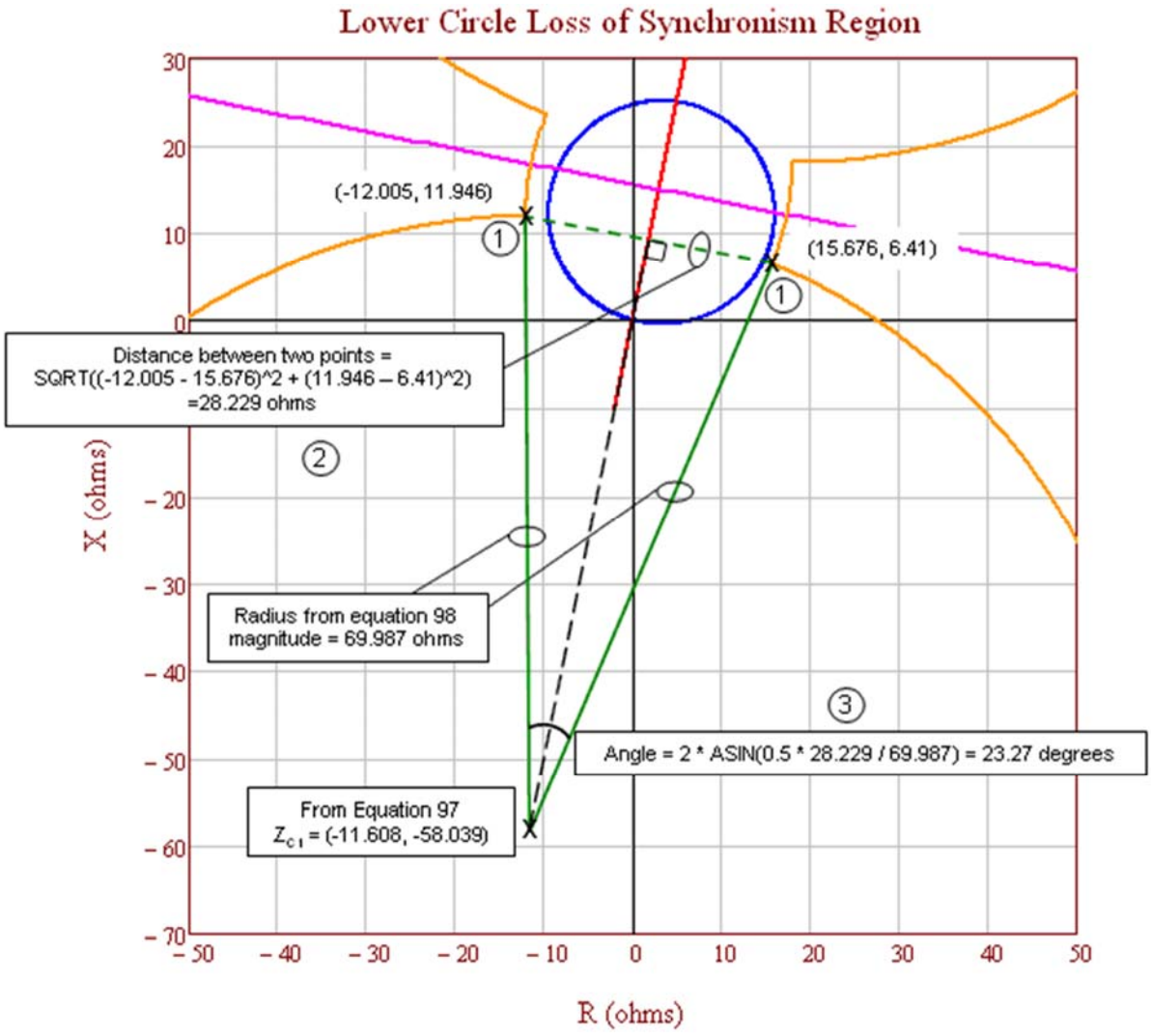


Figure 15b: Lower circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the lower circle loss-of-synchronism points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 0.7 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two lower circle loss-of-synchronism points identified in Step 1. 3) Calculate the angle of arc that connects the two lower circle loss-of-synchronism points identified in Step 1.

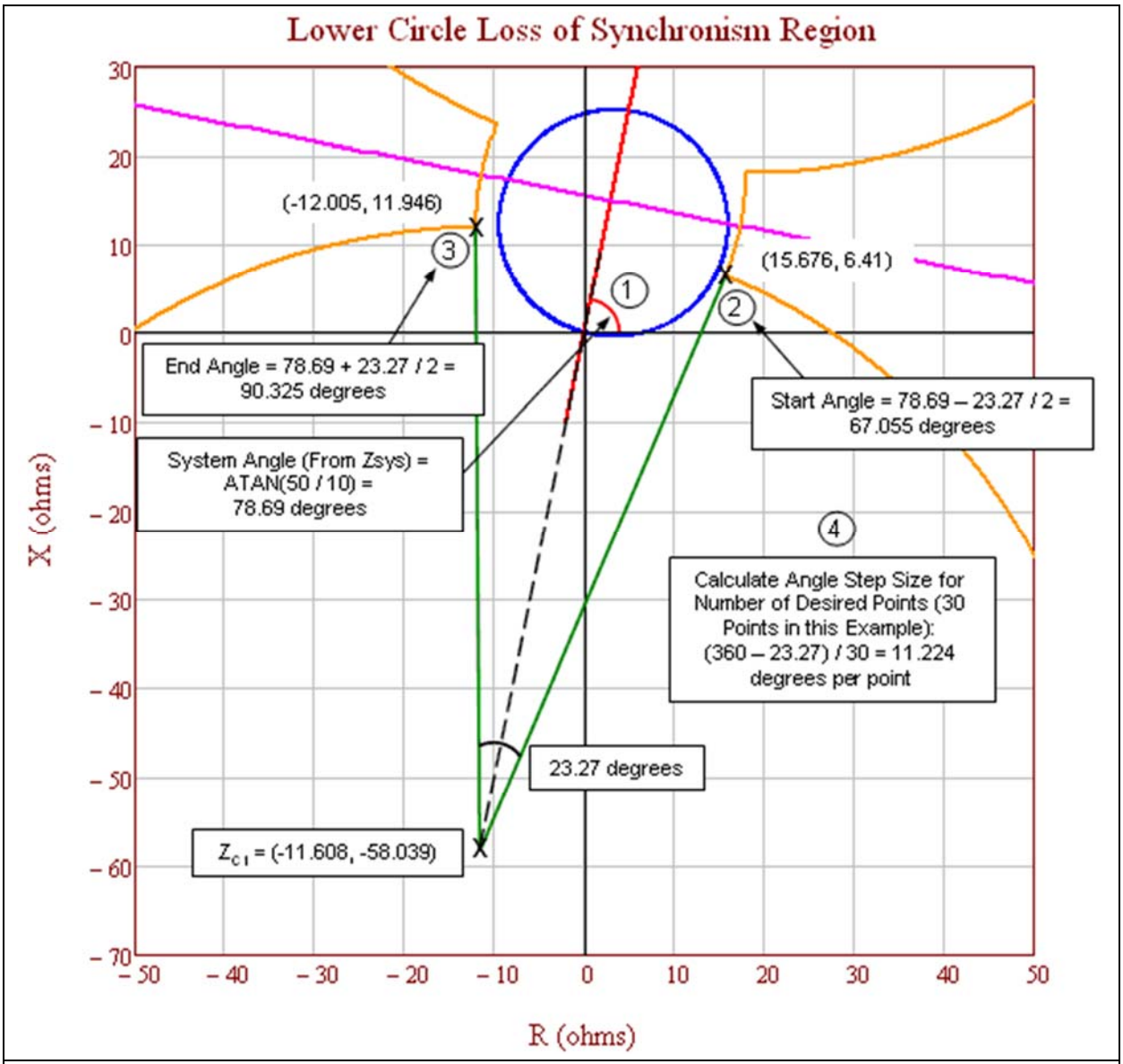


Figure 15c: Lower circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

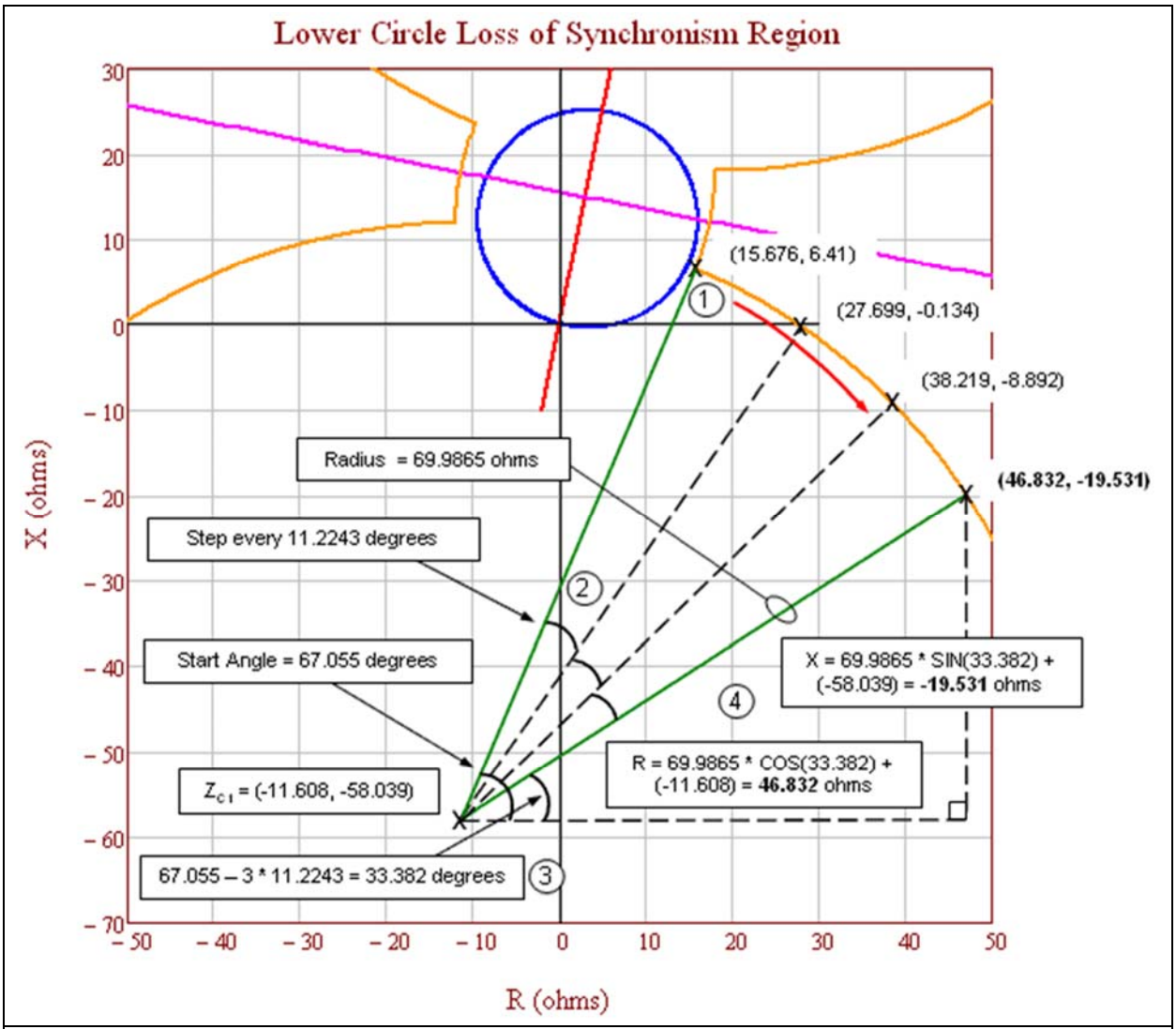


Figure 15d: Lower circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R–X coordinates.

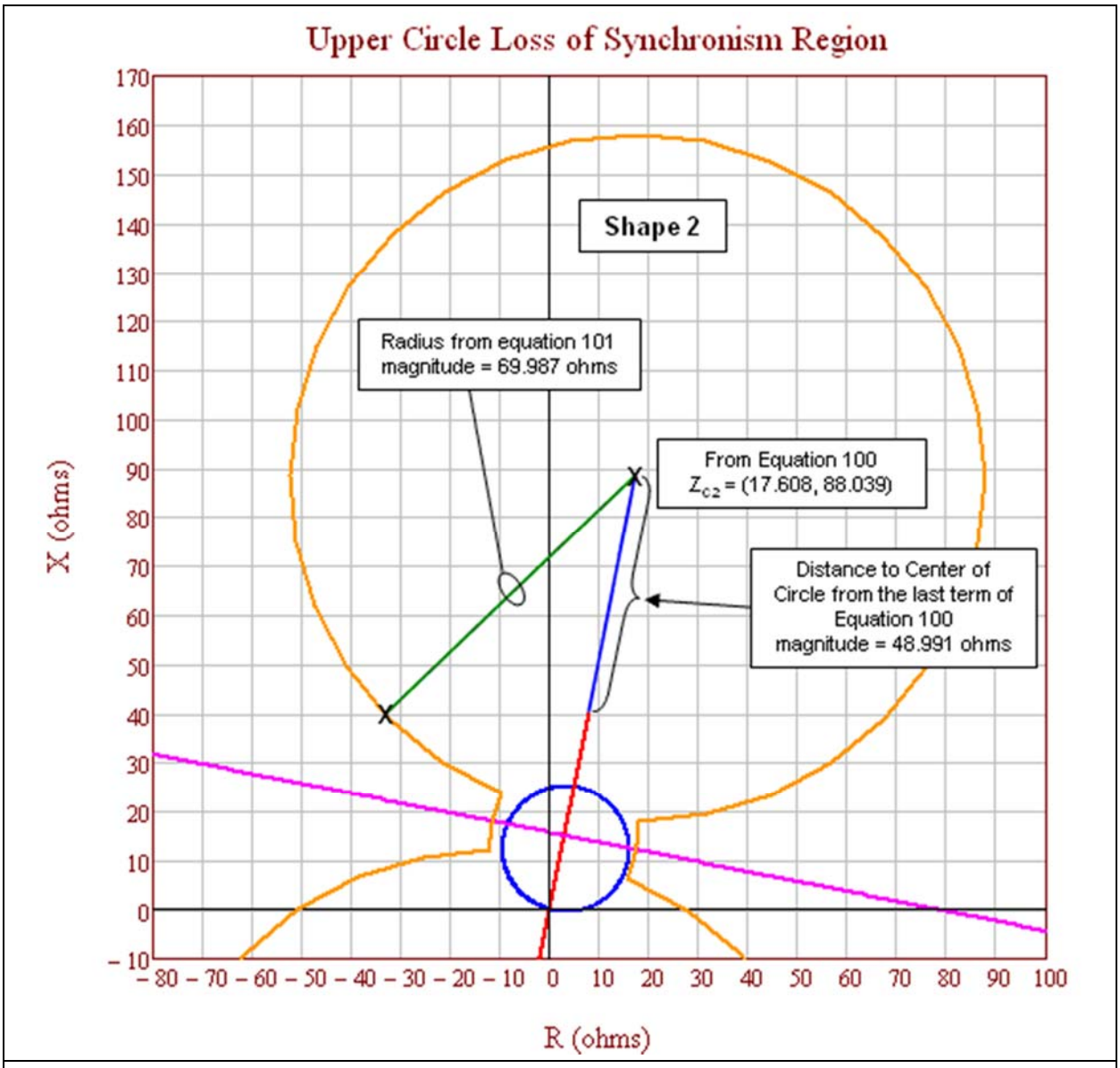


Figure 15e: Upper circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

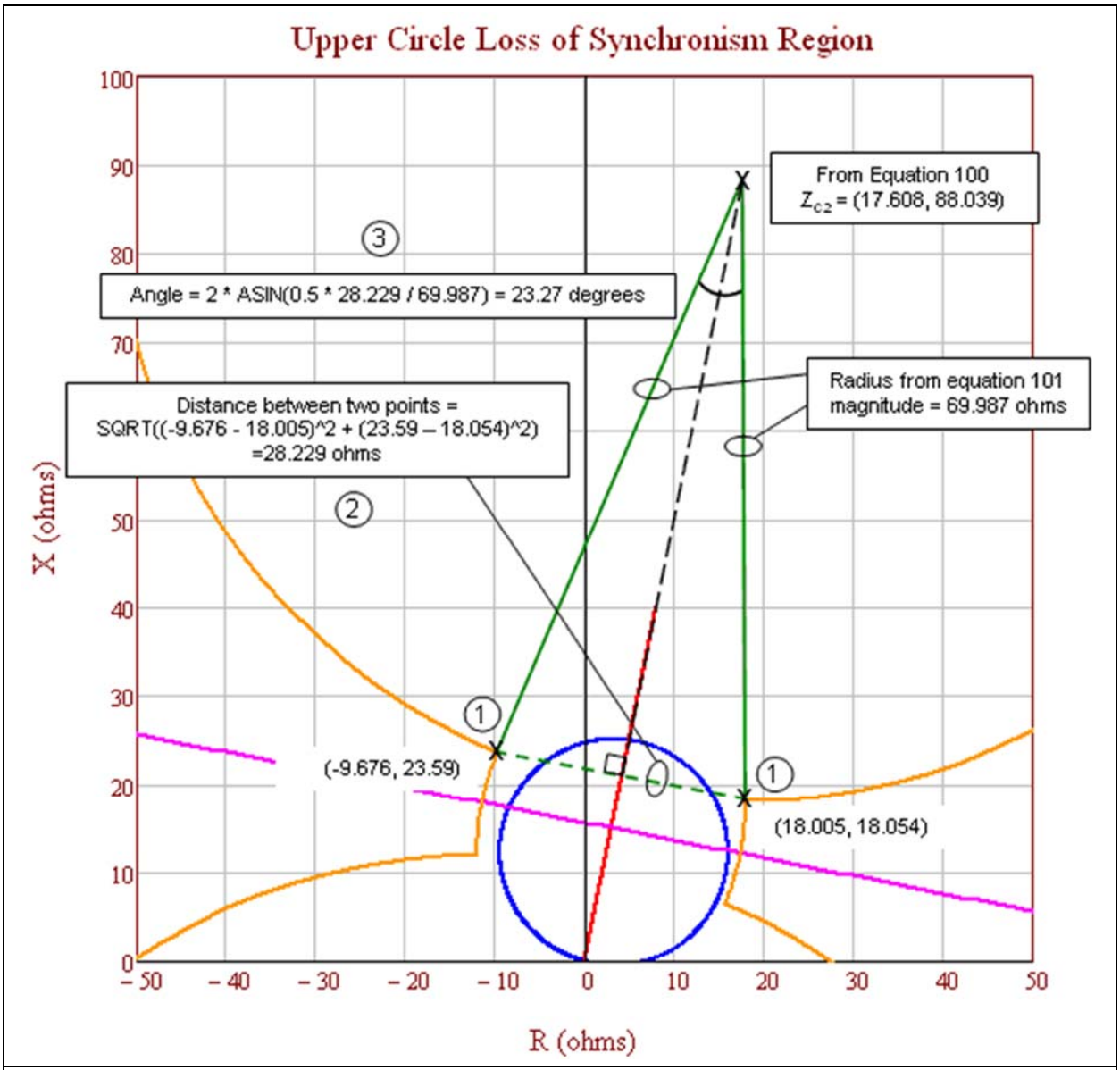


Figure 15f: Upper circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the upper circle points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 1.43 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two upper circle points identified in Step 1. 3) Calculate the angle of arc that connects the two upper circle points identified in Step 1.

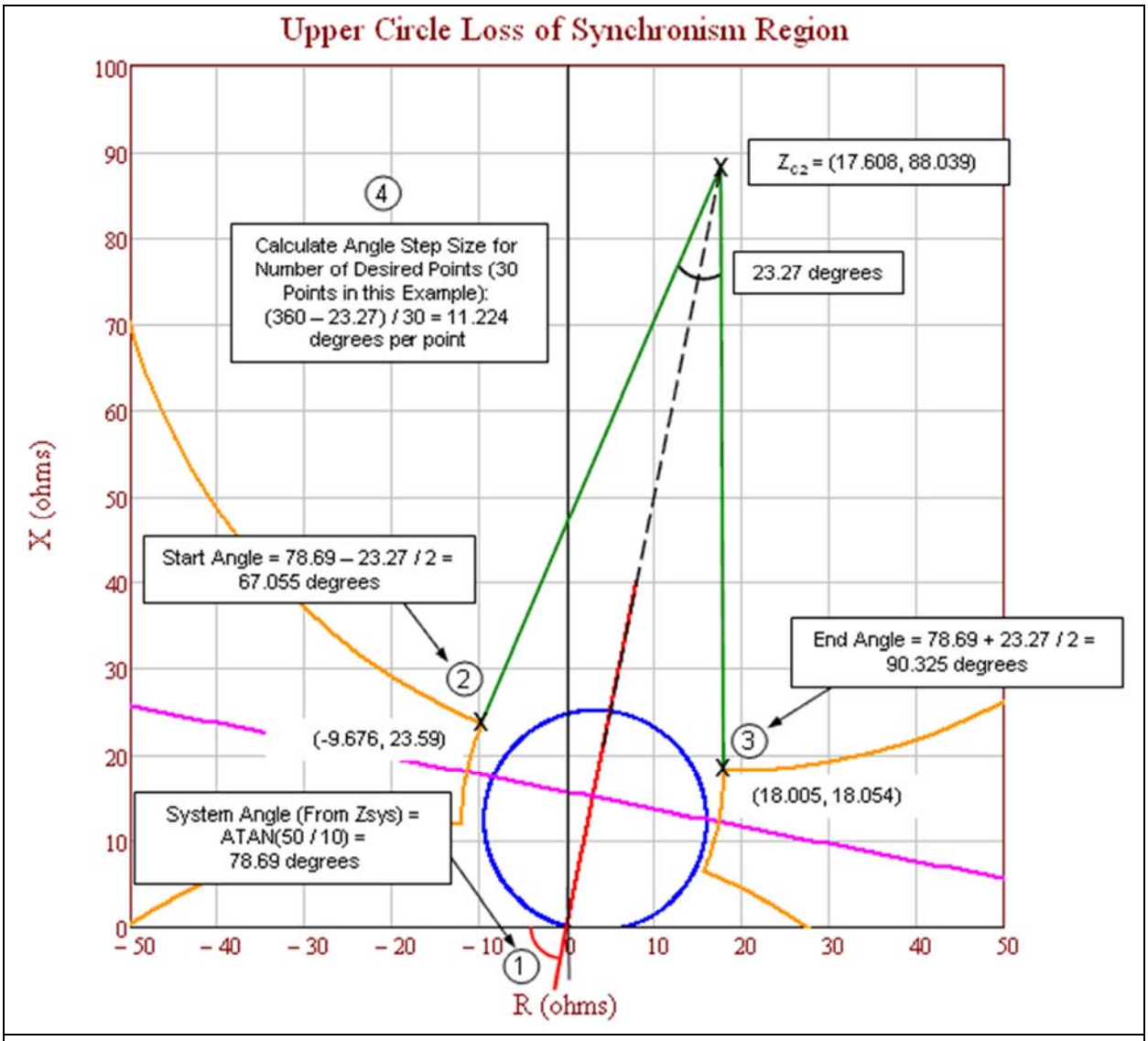


Figure 15g: Upper circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

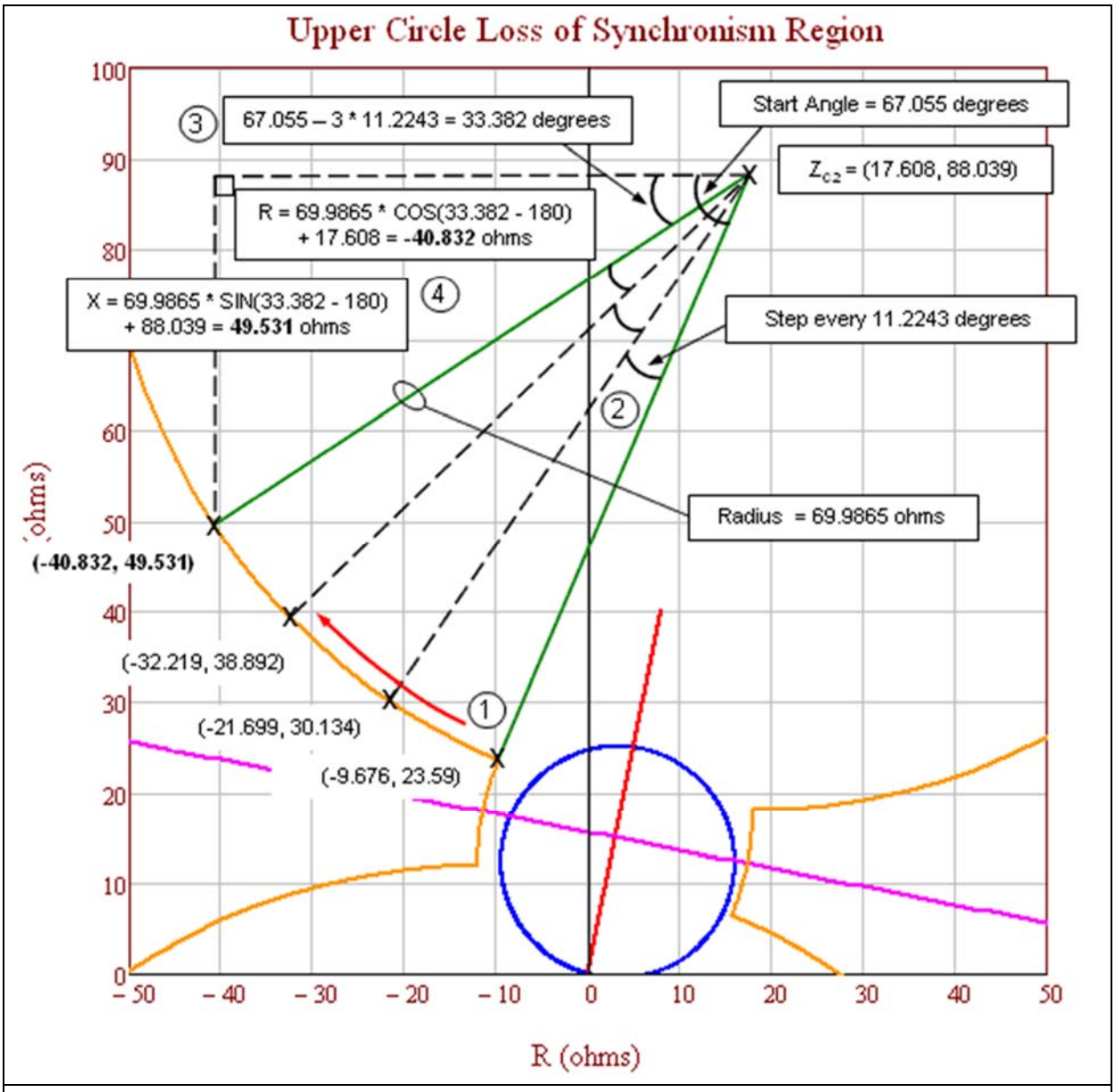


Figure 15h: Upper circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R-X coordinates.

Lower Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	15.676	6.41
55.831	27.699	-0.134
44.606	38.219	-8.892
33.382	**46.832**	**-19.531**
22.158	53.21	-31.643
10.933	57.108	-44.765
359.709	58.378	-58.395
348.485	56.97	-72.011
337.26	52.939	-85.092
326.036	46.438	-97.139
314.812	37.717	-107.69
303.587	27.109	-116.341
292.363	15.02	-122.762
281.139	1.913	-126.707
269.914	-11.712	-128.026
258.69	-25.333	-126.667
247.466	-38.429	-122.682
236.241	-50.499	-116.225
225.017	-61.081	-107.542
213.793	-69.771	-96.965
202.568	-76.235	-84.899
191.344	-80.227	-71.806
180.12	-81.594	-58.185
168.895	-80.284	-44.56
157.671	-76.347	-31.45
146.447	-69.933	-19.357
135.222	-61.288	-8.744
123.998	-50.742	-0.016
112.774	-38.699	6.491
101.549	-25.62	10.53
90.325	-12.005	11.946

Upper Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	-9.676	23.59
55.831	-21.699	30.134
44.606	-32.219	38.892
33.382	**-40.832**	**49.531**
22.158	-47.21	61.643
10.933	-51.108	74.765
359.709	-52.378	88.395
348.485	-50.97	102.011
337.26	-46.939	115.092
326.036	-40.438	127.139
314.812	-31.717	137.69
303.587	-21.109	146.341
292.363	-9.02	152.762
281.139	4.087	156.707
269.914	17.712	158.026
258.69	31.333	156.667
247.466	44.429	152.682
236.241	56.499	146.225
225.017	67.081	137.542
213.793	75.771	126.965
202.568	82.235	114.899
191.344	86.227	101.806
180.12	87.594	88.185
168.895	86.284	74.56
157.671	82.347	61.45
146.447	75.933	49.357
135.222	67.288	38.744
123.998	56.742	30.016
112.774	44.699	23.509
101.549	31.62	19.47
90.325	18.005	18.054

Figure 15i: Full tables of calculated lower and upper loss-of-synchronism circle coordinates. The highlighted row is the detailed calculated points in Figures 15d and 15h.

Application Specific to Criterion B

The PRC-026-1 – Attachment B, Criterion B evaluates overcurrent elements used for tripping. The same criteria as PRC-026-1 – Attachment B, Criterion A is used except for an additional criterion (No. 4) that calculates a current magnitude based upon generator internal voltage of 1.05 per unit. A value of 1.05 per unit generator voltage is used to establish a minimum pickup current value for overcurrent relays that have a time delay less than 15 cycles. The sending-end and receiving-end voltages are established at 1.05 per unit at 120 degree system separation angle. The 1.05 per unit is the typical upper end of the operating voltage, which is also consistent with the maximum power

transfer calculation using actual system source impedances in the PRC-023 NERC Reliability Standard. The formulas used to calculate the current are in Table 14 below.

Table 14: Example Calculation (Overcurrent)

This example is for a 230 kV line terminal with a directional instantaneous phase overcurrent element set to 50 amps secondary times a CT ratio of 160:1 that equals 8,000 amps, primary. The following calculation is where V_S equals the base line-to-ground sending-end generator source voltage times 1.05 at an angle of 120 degrees, V_R equals the base line-to-ground receiving-end generator internal voltage times 1.05 at an angle of 0 degrees, and Z_{sys} equals the sum of the sending-end source, line, and receiving-end source impedances in ohms. Here, the instantaneous phase setting of 8,000 amps is greater than the calculated system current of 5,716 amps; therefore, it meets PRC-026-1 – Attachment B, Criterion B.			
Eq. (102)	$V_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 1.05$		
	$V_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}} \times 1.05$		
	$V_S = 139{,}430\angle 120°\ V$		
Receiving-end generator terminal voltage.			
Eq. (103)	$V_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 1.05$		
	$V_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 1.05$		
	$V_R = 139{,}430\angle 0°\ V$		
The total impedance of the system (Z_{sys}) equals the sum of the sending-end source impedance (Z_S), the impedance of the line (Z_L), and receiving-end impedance (Z_R) in ohms.			
Given:	$Z_S = 3 + j26\ \Omega$	$Z_L = 1.3 + j8.7\ \Omega$	$Z_R = 0.3 + j7.3\ \Omega$
Eq. (104)	$Z_{sys} = Z_S + Z_L + Z_R$		
	$Z_{sys} = (3 + j26)\ \Omega + (1.3 + j8.7)\ \Omega + (0.3 + j7.3)\ \Omega$		
	$Z_{sys} = 4.6 + j42\ \Omega$		
Total system current.			
Eq. (105)	$I_{sys} = \frac{(V_S - V_R)}{Z_{sys}}$		
	$I_{sys} = \frac{(139{,}430\angle 120°\ V - 139{,}430\angle 0°\ V)}{(4.6 + j42)\ \Omega}$		
	$I_{sys} = 5{,}715.82\angle 66.25°\ A$		

Application Specific to Three-Terminal Lines

If a three-terminal line is identified as an Element that is susceptible to a power swing based on Requirement R1, the load-responsive protective relays at each end of the three-terminal line must be evaluated.

As shown in Figure 15j, the source impedances at each end of the line can be obtained from the similar short circuit calculation as for the two-terminal line (assuming the parallel transfer impedances are ignored).

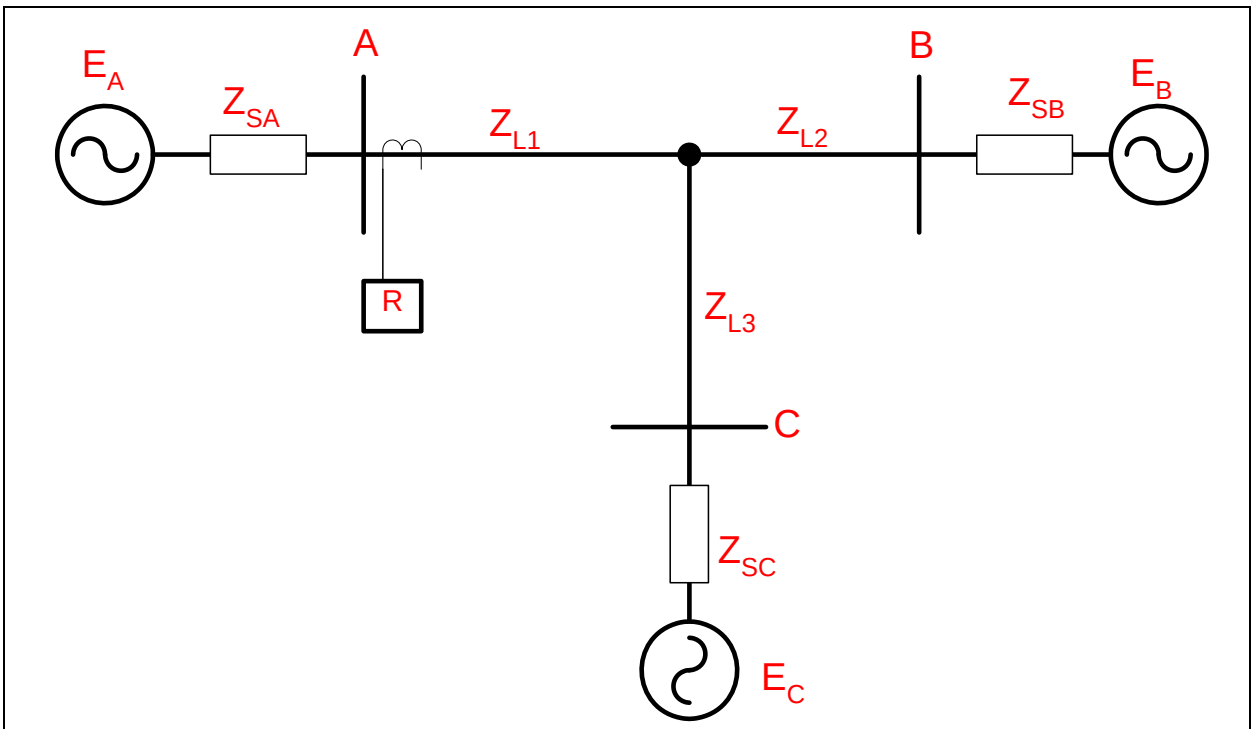


Figure 15j: Three-terminal line. To evaluate the load-responsive protective relays on the three-terminal line at Terminal A, the circuit in Figure 15j is first reduced to the equivalent circuit shown in Figure 15k. The evaluation process for the load-responsive protective relays on the line at Terminal A will now be the same as that of the two-terminal line.

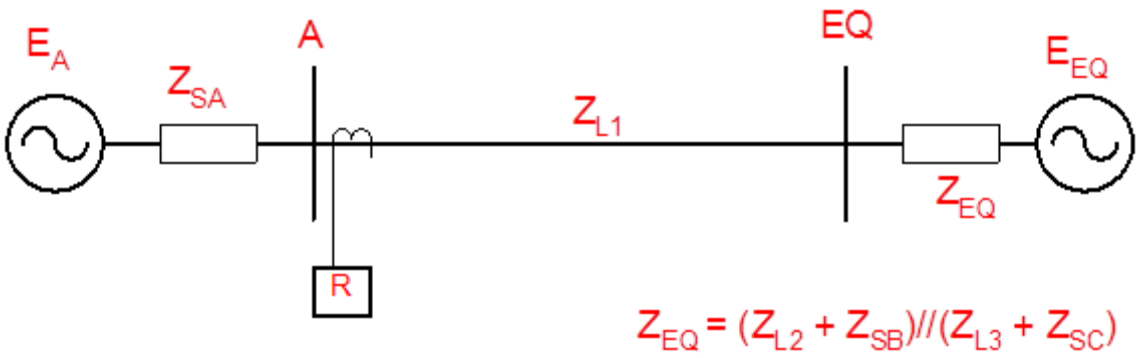


Figure 15k: Three-terminal line reduced to a two-terminal line.

Application to Generation Elements

As with transmission BES Elements, the determination of the apparent impedance seen at an Element located at, or near, a generation Facility is complex for power swings due to various interdependent quantities. These variances in quantities are caused by changes in machine internal voltage, speed governor action, voltage regulator action, the reaction of other local generators, and the reaction of other interconnected transmission BES Elements as the event progresses through the time domain. Though transient stability simulations may be used to determine the apparent impedance for verifying load-responsive relay settings,[18,19] Requirement R2, PRC-026-1 – Attachment B, Criteria A and B provides a simplified method for evaluating the load-responsive protective relay's susceptibility to tripping in response to a stable power swing without requiring stability simulations.

In general, the electrical center will be in the transmission system for cases where the generator is connected through a weak transmission system (high external impedance). In other cases where the generator is connected through a strong transmission system, the electrical center could be inside the unit connected zone.[20] In either case, load-responsive protective relays connected at the generator terminals or at the high-voltage side of the generator step-up (GSU) transformer may be challenged by power swings. Relays that may be challenged by power swings will be determined by the Planning Coordinator in Requirement R1 or by the Generator Owner after becoming aware of a generator, transformer, or transmission line BES Element that tripped[21] in response to a stable or unstable power swing due to the operation of its protective relay(s) in Requirement R2.

[18] Donald Reimert, *Protective Relaying for Power Generation Systems*, Boca Raton, FL, CRC Press, 2006.

[19] Prabha Kundur, *Power System Stability and Control*, EPRI, McGraw Hill, Inc., 1994.

[20] Ibid, Kundur.

[21] See Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing,"

Voltage controlled time-overcurrent and voltage-restrained time-overcurrent relays are excluded from this standard. When these relays are set based on equipment permissible overload capability, their operating times are much greater than 15 cycles for the current levels observed during a power swing.

Instantaneous overcurrent, time-overcurrent, and definite-time overcurrent relays with a time delay of less than 15 cycles for the current levels observed during a power swing are applicable and are required to be evaluated for identified Elements.

The generator loss-of-field protective function is provided by impedance relay(s) connected at the generator terminals. The settings are applied to protect the generator from a partial or complete loss of excitation under all generator loading conditions and, at the same time, be immune to tripping on stable power swings. It is more likely that the loss-of-field relay would operate during a power swing when the automatic voltage regulator (AVR) is in manual mode rather than when in automatic mode.[22] Figure 16 illustrates the loss-of-field relay in the R-X plot, which typically includes up to three zones of protection.

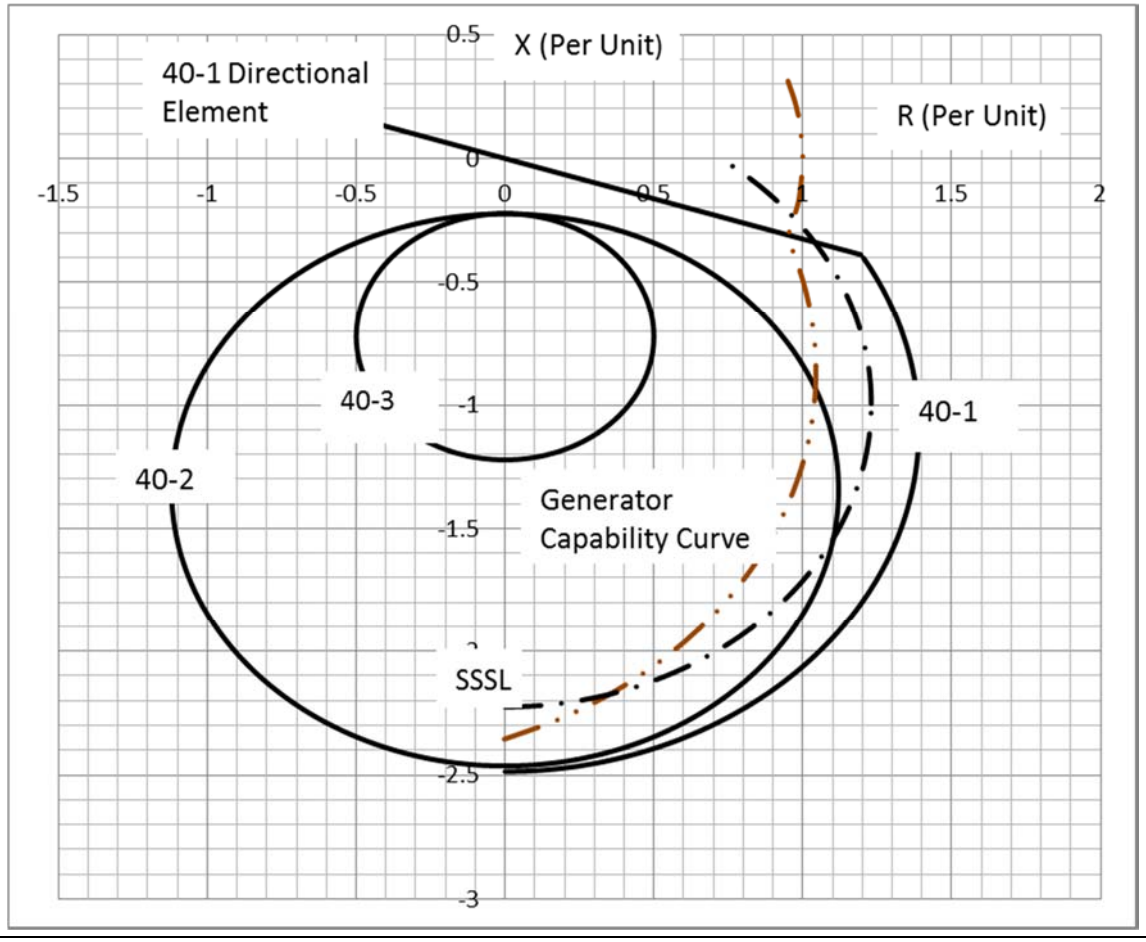


Figure 16: An R-X graph of typical impedance settings for loss-of-field relays.

[22] John Burdy, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

Loss-of-field characteristic 40-1 has a wider impedance characteristic (positive offset) than characteristic 40-2 or characteristic 40-3 and provides additional generator protection for a partial loss of field or a loss of field under low load (less than 10% of rated). The tripping logic of this protection scheme is established by a directional contact, a voltage setpoint, and a time delay. The voltage and time delay add security to the relay operation for stable power swings. Characteristic 40-3 is less sensitive to power swings than characteristic 40-2 and is set outside the generator capability curve in the leading direction. Regardless of the relay impedance setting, PRC-019[23] requires that the "in-service limiters operate before Protection Systems to avoid unnecessary trip" and "in-service Protection System devices are set to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits." Time delays for tripping associated with loss-of-field relays[24,25] have a range from 15 cycles for characteristic 40-2 to 60 cycles for characteristic 40-1 to minimize tripping during stable power swings. In PRC-026-1, 15 cycles establishes a threshold for applicability; however, it is the responsibility of the Generator Owner to establish settings that provide security against stable power swings and, at the same time, dependable protection for the generator.

The simple two-machine system circuit (method also used in the Application to Transmission Elements section) is used to analyze the effect of a power swing at a generator facility for load-responsive relays. In this section, the calculation method is used for calculating the impedance seen by the relay connected at a point in the circuit.[26] The electrical quantities used to determine the apparent impedance plot using this method are generator saturated transient reactance (X'_d), GSU transformer impedance (X_{GSU}), transmission line impedance (Z_L), and the system equivalent (Z_e) at the point of interconnection. All impedance values are known to the Generator Owner except for the system equivalent. The system equivalent is obtainable from the Transmission Owner. The sending-end and receiving-end source voltages are varied from 0.0 to 1.0 per unit to form the lens shape portion of the unstable power swing region. The voltage range of 0.7 to 1.0 results in a ratio range from 0.7 to 1.43. This ratio range is used to form the lower and upper loss-of-synchronism circle shapes of the unstable power swing region. A system separation angle of 120 degrees is used in accordance with PRC-026-1 – Attachment B criteria for each load-responsive protective relay evaluation.

Table 15 below is an example calculation of the apparent impedance locus method based on Figures 17 and 18.[27] In this example, the generator is connected to the 345 kV transmission system through the GSU transformer and has the listed ratings. Note that the load-responsive protective relays in this example may have ownership with the Generator Owner or the Transmission Owner.

[23] Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

[24] Ibid, Burdy.

[25] *Applied Protective Relaying*, Westinghouse Electric Corporation, 1979.

[26] Edward Wilson Kimbark, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

[27] Ibid, Kimbark.

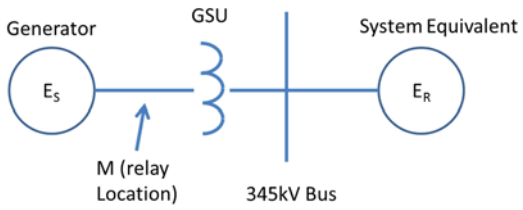


Figure 17: Simple one-line diagram of the system to be evaluated.

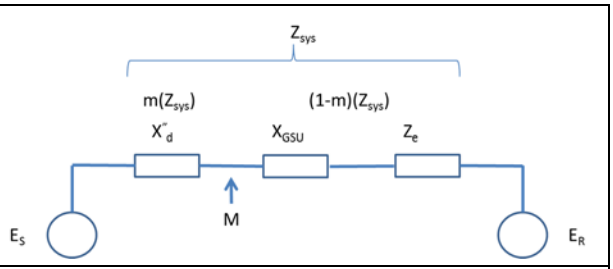


Figure 18: Simple system equivalent impedance diagram to be evaluated.[28]

Table15: Example Data (Generator)	
Input Descriptions	**Input Values**
Synchronous Generator nameplate (MVA)	940 MVA
Saturated transient reactance (940 MVA base)	$X'_d = 0.3845$ per unit
Generator rated voltage (Line-to-Line)	$20\ kV$
Generator step-up (GSU) transformer rating	$880\ MVA$
GSU transformer reactance (880 MVA base)	$X_{GSU} = 16.05\%$
System Equivalent (100 MVA base)	$Z_e = 0.00723\angle 90°$ per unit
Generator Owner Load-Responsive Protective Relays	
40-1	Positive Offset Impedance
	Offset = 0.294 per unit
	Diameter = 0.294 per unit
40-2	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 2.24 per unit
40-3	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 1.00 per unit
21-1	Diameter = 0.643 per unit
	MTA = 85°

[28] Ibid, Kimbark.

Table15: Example Data (Generator)	
50	I (pickup) = 5.0 per unit
Transmission Owned Load-Responsive Protective Relays	
21-2	Diameter = 0.55 per unit
	MTA = 85°

Calculations shown for a 120 degree angle and $E_S/E_R = 1$. The equation for calculating Z_R is:[29]

Eq. (106) $$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$$

Where m is the relay location as a function of the total impedance (real number less than 1)

E_S and E_R is the sending-end and receiving-end voltages

Z_{sys} is the total system impedance

Z_R is the complex impedance at the relay location and plotted on an R-X diagram

All of the above are constants (940 MVA base) while the angle δ is varied. Table 16 below contains calculations for a generator using the data listed in Table 15.

Table16: Example Calculations (Generator)			
The following calculations are on a 940 MVA base.			
Given:	$X'_d = j0.3845\ pu$	$X_{GSU} = j0.17144\ pu$	$Z_e = j0.06796\ pu$
Eq. (107)	$Z_{sys} = X'_d + X_{GSU} + Z_e$		
	$Z_{sys} = j0.3845\ pu + j0.17144\ pu + j0.06796\ pu$		
	$Z_{sys} = 0.6239\ \angle 90°\ pu$		
Eq. (108)	$m = \frac{X'_d}{Z_{sys}} = \frac{0.3845}{0.6239} = 0.6163$		
Eq. (109)	$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$		
	$Z_R = \left(\frac{(1-0.6163) \times (1\angle 120°) + (0.6163)(1\angle 0°)}{1\angle 120° - 1\angle 0°}\right) \times (0.6239\angle 90°)\ pu$		

[29] Ibid, Kimbark.

Table16: Example Calculations (Generator)	
	$Z_R = \left(\frac{0.4244 + j0.3323}{-1.5 + j\ 0.866}\right) \times (0.6239\angle 90°)\ pu$
	$Z_R = (0.3116 \angle -111.95°) \times (0.6239\angle 90°)\ pu$
	$Z_R = 0.194 \angle -21.95°\ pu$
	$Z_R = -0.18 - j0.073\ pu$

Table 17 lists the swing impedance values at other angles and at E_S/E_R = 1, 1.43, and 0.7. The impedance values are plotted on an R-X graph with the center being at the generator terminals for use in evaluating impedance relay settings.

Table 17: Sample Calculations for a Swing Impedance Chart for Varying Voltages at the Sending-End and Receiving-End.

	E_S/E_R=1		E_S/E_R=1.43		E_S/E_R=0.7	
	Z_R		Z_R		Z_R	
Angle (δ) (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)
90	0.320	-13.1	0.296	6.3	0.344	-31.5
120	0.194	-21.9	0.173	-0.4	0.227	-40.1
150	0.111	-41.0	0.082	-10.3	0.154	-58.4
210	0.111	-25.9	0.082	190.3	0.154	238.4
240	0.194	201.9	0.173	180.4	0.225	220.1
270	0.320	193.1	0.296	173.7	0.344	211.5

Requirement R2 Generator Examples

Distance Relay Application

Based on PRC-026-1 – Attachment B, Criterion A, the distance relay (21-1) (i.e., owned by the Generation Owner) characteristic is in the region where a stable power swing would not occur as shown in Figure 19. There is no further obligation to the owner in this standard for this load-responsive protective relay.

The distance relay (21-2) (i.e., owned by the Transmission Owner) is connected at the high-voltage side of the GSU transformer and its impedance characteristic is in the region where a stable power swing could occur causing the relay to operate. In this example, if the intentional time delay of this relay is less than 15 cycles, the PRC-026 – Attachment B, Criterion A cannot be met, thus the Transmission Owner is required to create a CAP (Requirement R3). Some of the options include,

but are not limited to, changing the relay setting (i.e., impedance reach, angle, time delay), modify the scheme (i.e., add PSB), or replace the Protection System. Note that the relay may be excluded from this standard if it has an intentional time delay equal to or greater than 15 cycles.

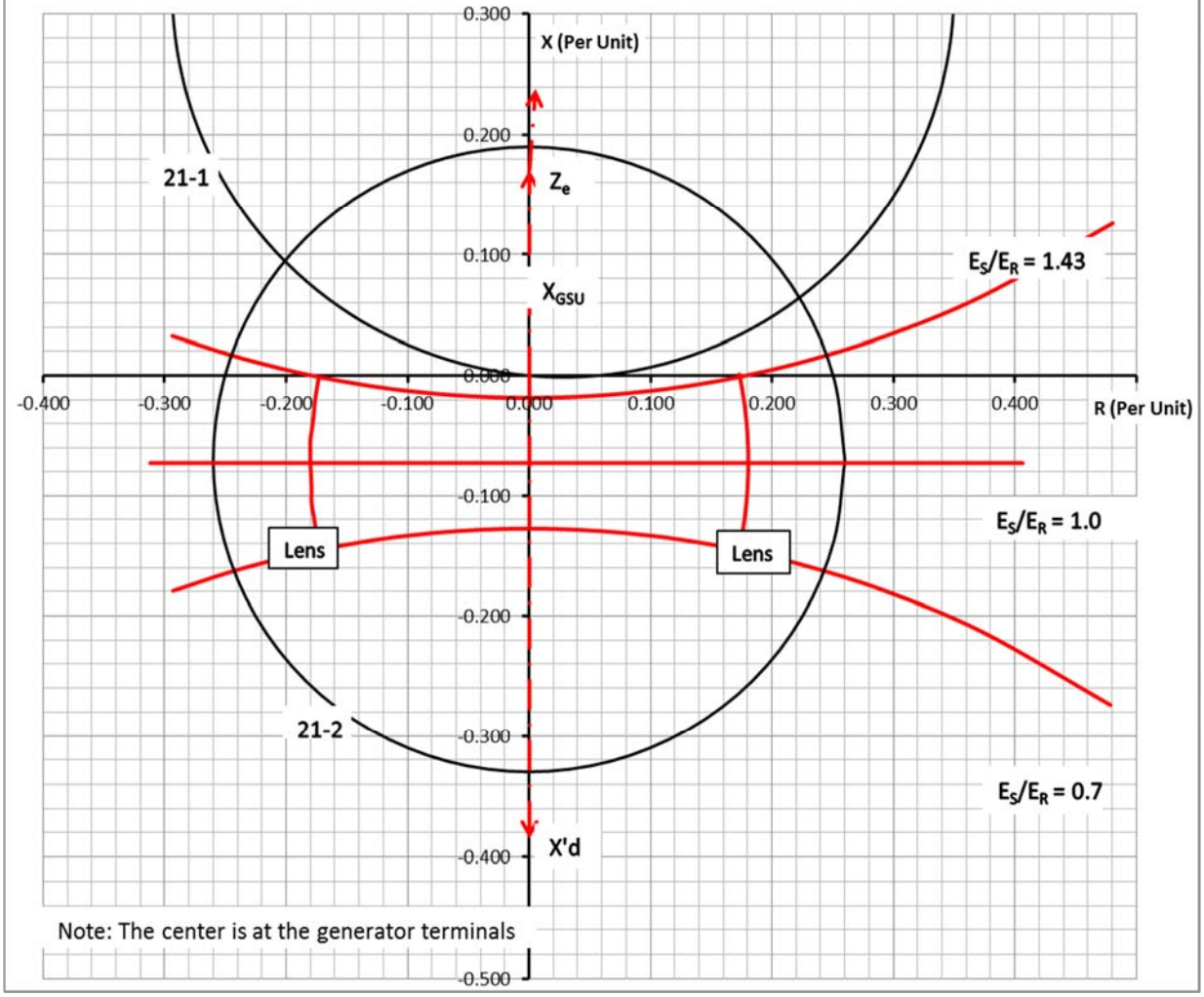


Figure 19: Swing impedance graph for impedance relays at a generating facility.

Loss-of-Field Relay Application

In Figure 20, the R-X diagram shows the loss-of-field relay (40-1 and 40-2) characteristics are in the region where a stable power swing can cause a relay operation. Protective relay 40-1 would be excluded if it has an intentional time delay equal to or greater than 15 cycles. Similarly, 40-2 would be excluded if its intentional time delay is equal to or greater than 15 cycles. For example, if 40-1 has a time delay of 1 second and 40-2 has a time delay of 0.25 seconds, they are excluded and there is no further obligation on the Generator Owner in this standard for these relays. The

loss-of-field relay characteristic 40-3 is entirely inside the unstable power swing region. In this case, the owner may select high speed tripping on operation of the 40-3 impedance element.

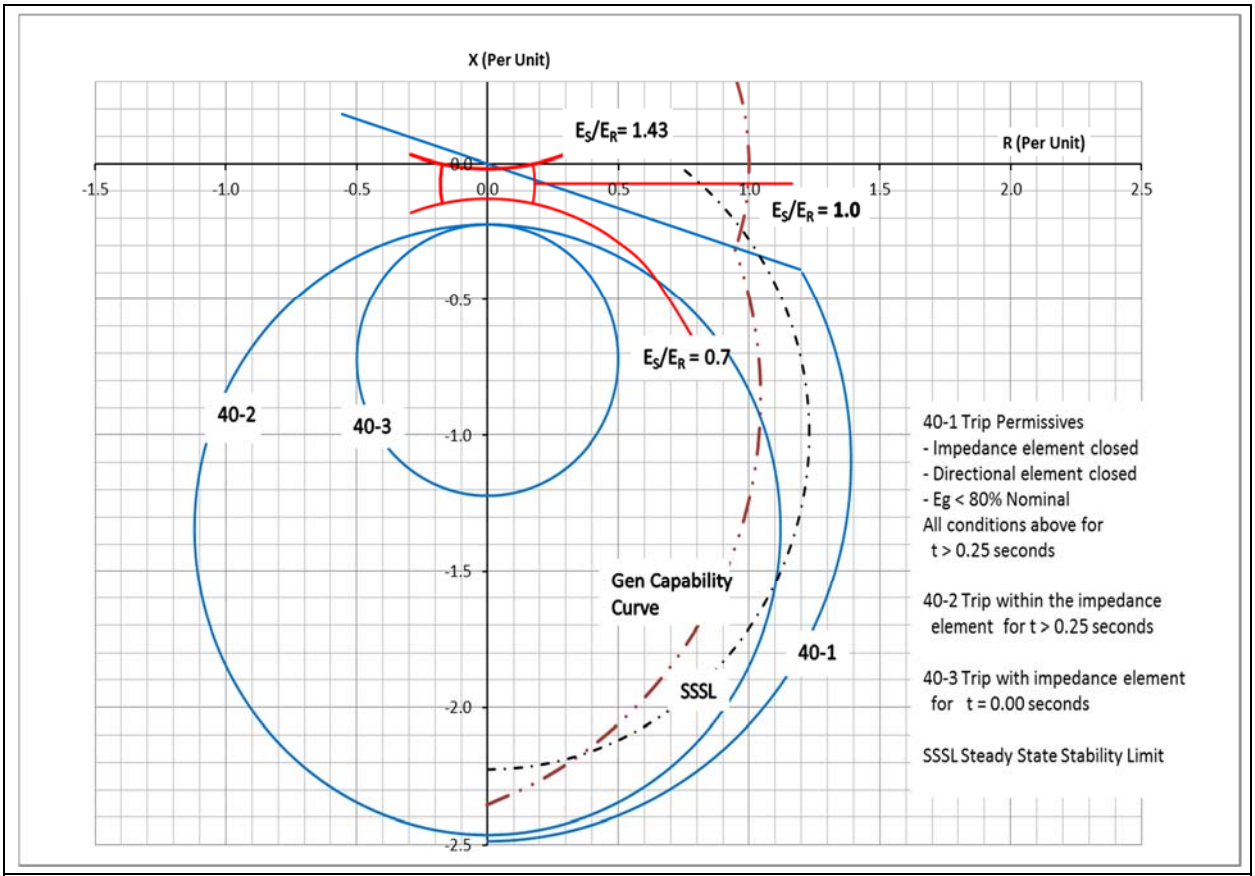


Figure 20: Typical R-X graph for loss-of-field relays with a portion of the unstable power swing region defined by PRC-026-1 – Attachment B, Criterion A.

Instantaneous Overcurrent Relay

In similar fashion to the transmission line overcurrent example calculation in Table 14, the instantaneous overcurrent relay minimum setting is established by PRC-026-1 – Attachment B, Criterion B. The solution is found by:

Eq. (110) $$I_{sys} = \frac{E_S - E_R}{Z_{\text{sys}}}$$

As stated in the relay settings in Table 15, the relay is installed on the high-voltage side of the GSU transformer with a pickup of 5.0 per unit. The maximum allowable current is calculated below.

$$I_{sys} = \frac{(1.05\angle 120° - 1.05\angle 0°)}{0.6239\angle 90°}\ pu$$

$$I_{sys} = \frac{1.819\angle 150°}{0.6239\angle 90°} pu$$

$$I_{sys} = 2.91\ \angle 60°\ pu$$

The instantaneous phase setting of 5.0 per unit is greater than the calculated system current of 2.91 per unit; therefore, it meets the PRC-026-1 – Attachment B, Criterion B.

Out-of-Step Tripping for Generation Facilities

Out-of-step protection for the generator generally falls into three different schemes. The first scheme is a distance relay connected at the high-voltage side of the GSU transformer with the directional element looking toward the generator. Because this relay setting may be the same setting used for generator backup protection (see Requirement R2 Generator Examples, Distance Relay Application), it is susceptible to tripping in response to stable power swings and would require modification. Because this scheme is susceptible to tripping in response to stable power swings and any modification to the mho circle will jeopardize the overall protection of the out-of-step protection of the generator, available technical literature does not recommend using this scheme specifically for generator out-of-step protection. The second and third out-of-step Protection System schemes are commonly referred to as single and double blinder schemes. These schemes are installed or enabled for out-of-step protection using a combination of blinders, a mho element, and timers. The combination of these protective relay functions provides out-of-step protection and discrimination logic for stable and unstable power swings. Single blinder schemes use logic that discriminate between stable and unstable power swings by issuing a trip command after the first slip cycle. Double blinder schemes are more complex than the single blinder scheme and, depending on the settings of the inner blinder, a trip for a stable power swing may occur. While the logic discriminates between stable and unstable power swings in either scheme, it is important that the trip initiating blinders be set at an angle greater than the stability limit of 120 degrees to remove the possibility of a trip for a stable power swing. Below is a discussion of the double blinder scheme.

Double Blinder Scheme

The double blinder scheme is a method for measuring the rate of change of positive sequence impedance for out-of-step swing detection. The scheme compares a timer setting to the actual elapsed time required by the impedance locus to pass between two impedance characteristics. In this case, the two impedance characteristics are simple blinders, each set to a specific resistive reach on the R-X plane. Typically, the two blinders on the left half plane are the mirror images of those on the right half plane. The scheme typically includes a mho characteristic which acts as a starting element, but is not a tripping element.

The scheme detects the blinder crossings and time delays as represented on the R-X plane as shown in Figure 21. The system impedance is composed of the generator transient (X_d'), GSU transformer (X_T), and transmission system (X_{system}), impedances.

The scheme logic is initiated when the swing locus crosses the outer Blinder R1 (Figure 21), on the right at separation angle α. The scheme only commits to take action when a swing crosses the

inner blinder. At this point the scheme logic seals in the out-of-step trip logic at separation angle β. Tripping actually asserts as the impedance locus leaves the scheme characteristic at separation angle δ.

The power swing may leave both inner and outer blinders in either direction, and tripping will assert. Therefore, the inner blinder must be set such that the separation angle β is large enough that the system cannot recover. This angle should be set at 120 degrees or more. Setting the angle greater than 120 degrees satisfies the PRC-026-1 – Attachment B, Criterion A (No. 1, 1st bullet) since the tripping function is asserted by the blinder element. Transient stability studies may indicate that a smaller stability limit angle is acceptable under PRC-026-1 – Attachment B, Criterion A (No. 1, 2nd bullet). In this respect, the double blinder scheme is similar to the double lens and triple lens schemes and many transmission application out-of-step schemes.

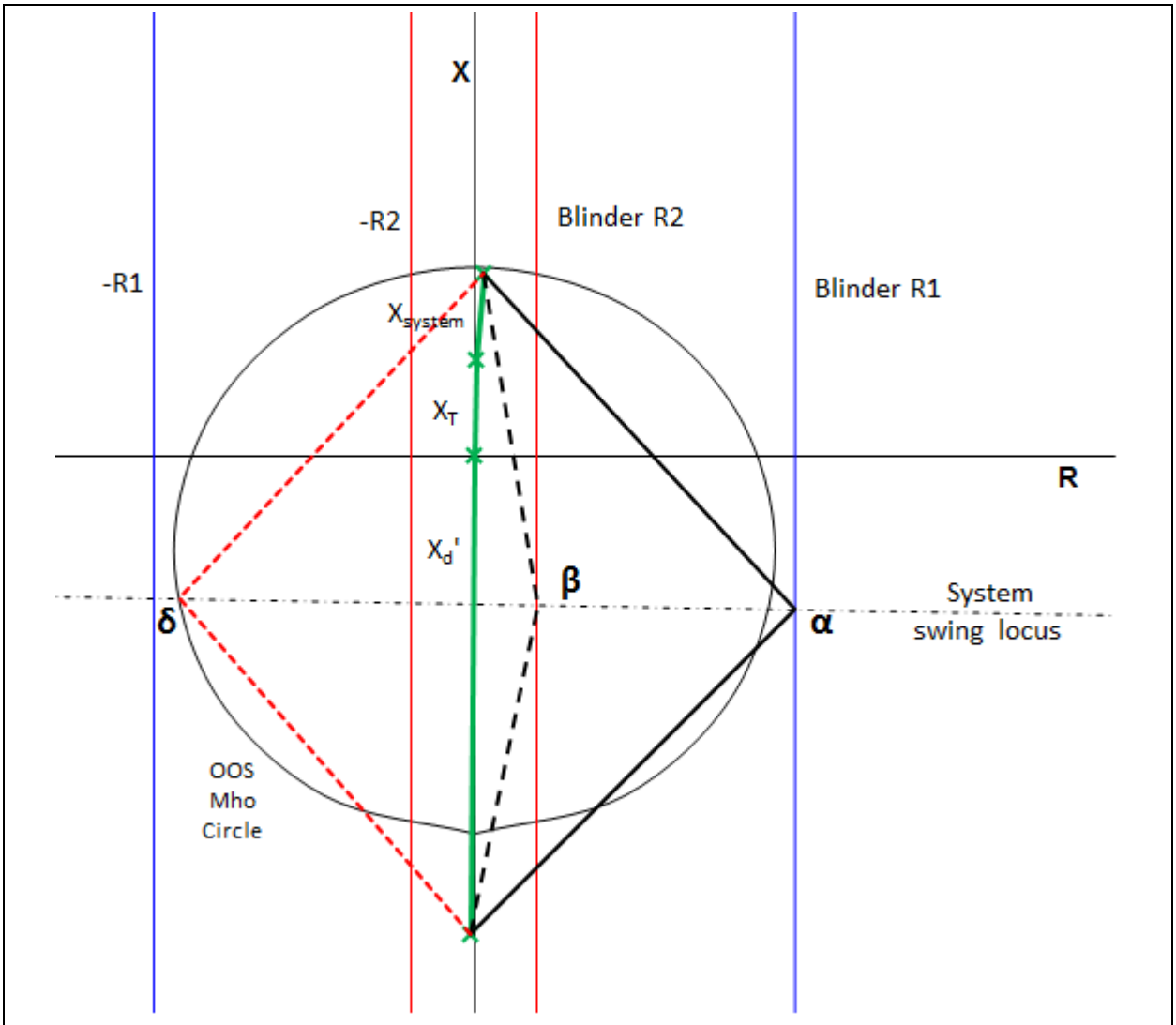


Figure 21: Double Blinder Scheme generic out of step characteristics.

Figure 22 illustrates a sample setting of the double blinder scheme for the example 940 MVA generator. The only setting requirement for this relay scheme is the right inner blinder, which must be set greater than the separation angle of 120 degrees (or a lesser angle based on a transient stability study) to ensure that the out-of-step protective function is expected to not trip in response to a stable power swing during non-Fault conditions. Other settings such as the mho characteristic, outer blinders, and timers are set according to transient stability studies and are not a part of this standard.

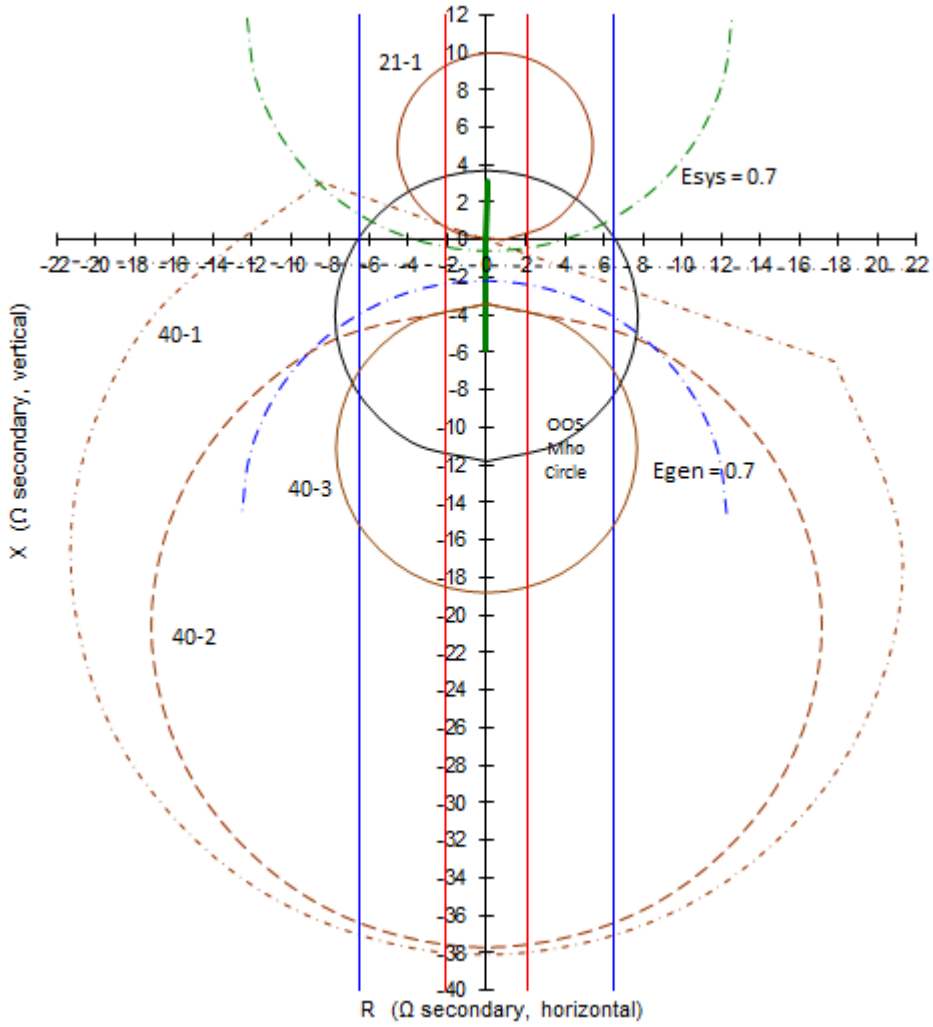


Figure 22: Double Blinder Out-of-Step Scheme with unit impedance data and load-responsive protective relay impedance characteristics for the example 940 MVA generator, scaled in relay secondary ohms.

Requirement R3

To achieve the stated purpose of this standard, which is to ensure that relays are expected to not trip in response to stable power swings during non-Fault conditions, this Requirement ensures that the applicable entity develops a Corrective Action Plan (CAP) that reduces the risk of relays tripping in response to a stable power swing during non-Fault conditions that may occur on any applicable BES Element.

Requirement R4

To achieve the stated purpose of this standard, which is to ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions, the applicable entity is required to implement any CAP developed pursuant to Requirement R3 such that the Protection System will meet PRC-026-1 – Attachment B criteria or can be excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element). Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until all actions are complete. Accomplishing this objective is intended to reduce the occurrence of Protection System tripping during a stable power swing, thereby improving reliability and minimizing risk to the BES.

The following are examples of actions taken to complete CAPs for a relay that did not meet PRC-026-1 – Attachment B and could be at-risk of tripping in response to a stable power swing during non-Fault conditions. A Protection System change was determined to be acceptable (without diminishing the ability of the relay to protect for faults within its zone of protection).

> **Example R4a:** Actions: Settings were issued on 6/02/2015 to reduce the Zone 2 reach of the impedance relay used in the directional comparison unblocking (DCUB) scheme from 30 ohms to 25 ohms so that the relay characteristic is completely contained within the lens characteristic identified by the criterion. The settings were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.
>
> **Example R4b:** Actions: Settings were issued on 6/02/2015 to enable out-of-step blocking on the existing microprocessor-based relay to prevent tripping in response to stable power swings. The setting changes were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.

The following is an example of actions taken to complete a CAP for a relay responding to a stable power swing that required the addition of an electromechanical power swing blocking relay.

> **Example R4c:** Actions: A project for the addition of an electromechanical power swing blocking relay to supervise the Zone 2 impedance relay was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The relay installation was completed on 9/25/2015. CAP was completed on 9/25/2015.

The following is an example of actions taken to complete a CAP with a timetable that required updating for the replacement of the relay.

> **Example R4d:** Actions: A project for the replacement of the impedance relays at both terminals of line X with line current differential relays was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The completion of the project was postponed due to line outage rescheduling from 11/15/2015 to 3/15/2016. Following the timetable change, the impedance relay replacement was completed on 3/18/2016. CAP was completed on 3/18/2016.

The CAP is complete when all the documented actions to remedy the specific problem (i.e., unnecessary tripping during stable power swings) are completed.

Justification for Including Unstable Power Swings in the Requirements

Protection Systems that are applicable to the Standard and must be secure for a stable power swing condition (i.e., meets PRC-026-1 – Attachment B criteria) are identified based on Elements that are susceptible to both stable and unstable power swings. This section provides an example of why Elements that trip in response to unstable power swings (in addition to stable power swings) are identified and that their load-responsive protective relays need to be evaluated under PRC-026-1 – Attachment B criteria.

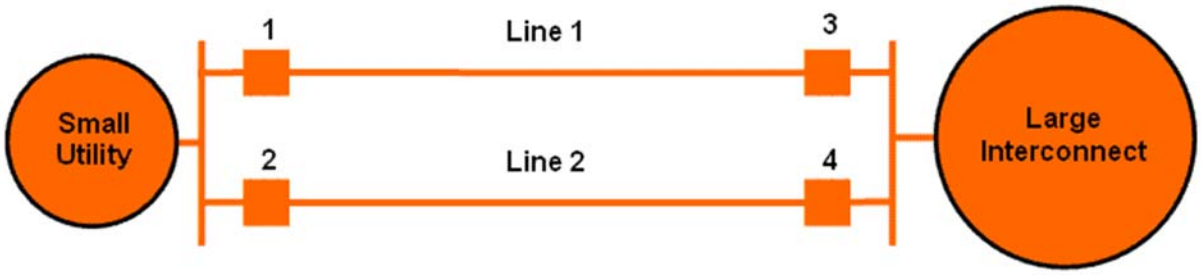


Figure 23: A simple electrical system where two lines tie a small utility to a much larger interconnection.

In Figure 23 the relays at circuit breakers 1, 2, 3, and 4 are equipped with a typical overreaching Zone 2 pilot system, using a Directional Comparison Blocking (DCB) scheme. Internal faults (or power swings) will result in instantaneous tripping of the Zone 2 relays if the measured fault or power swing impedance falls within the zone 2 operating characteristic. These lines will trip on

pilot Zone 2 for out-of-step conditions if the power swing impedance characteristic enters into Zone 2. All breakers are rated for out-of-phase switching.

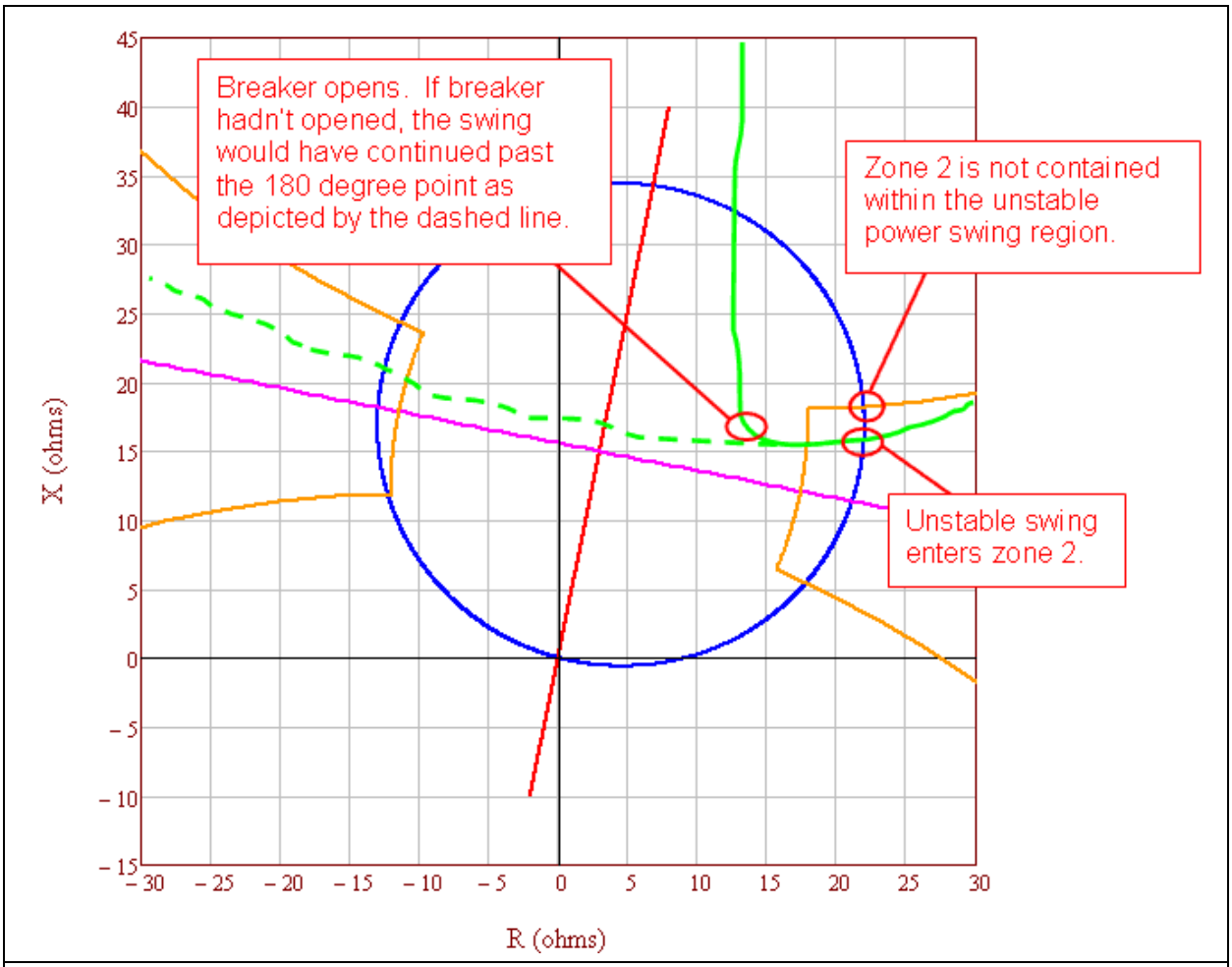


Figure 24: In this case, the Zone 2 element on circuit breakers 1, 2, 3, and 4 did not meet the PRC-026-1 – Attachment B criteria (this figure depicts the power swing as seen by relays on breakers 3 and 4).

In Figure 24, a large disturbance occurs within the small utility and its system goes out-of-step with the large interconnect. The small utility is importing power at the time of the disturbance. The actual power swing, as shown by the solid green line, enters the Zone 2 relay characteristic on the terminals of Lines 1, 2, 3, and 4 causing both lines to trip as shown in Figure 25.

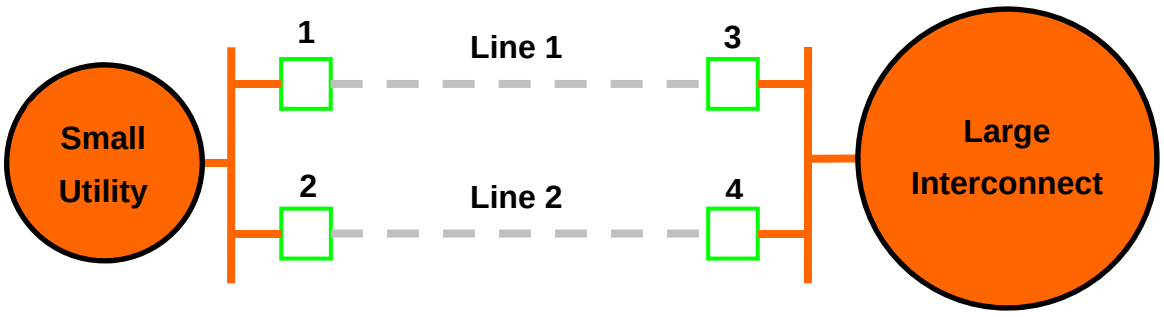


Figure 25: Islanding of the small utility due to Lines 1 and 2 tripping in response to an unstable power swing.

In Figure 25, the relays at circuit breakers 1, 2, 3, and 4 have correctly tripped due to the unstable power swing (shown by the dashed green line in Figure 24), de-energizing Lines 1 and 2, and creating an island between the small utility and the big interconnect. The small utility shed 500 MW of load on underfrequency and maintained a load to generation balance.

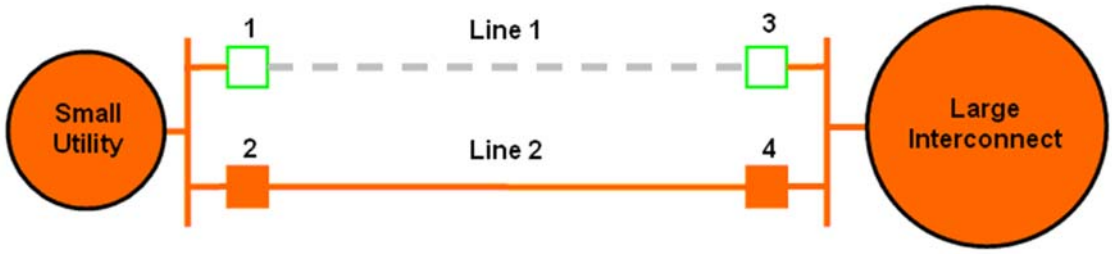


Figure 26: Line 1 is out-of-service for maintenance, Line 2 is loaded beyond its normal rating (but within its emergency rating).

Subsequent to the correct tripping of Lines 1 and 2 for the unstable power swing in Figure 25, another system disturbance occurs while the system is operating with Line 1 out-of-service for maintenance. The disturbance causes a stable power swing on Line 2, which challenges the relays at circuit breakers 2 and 4 as shown in Figure 27.

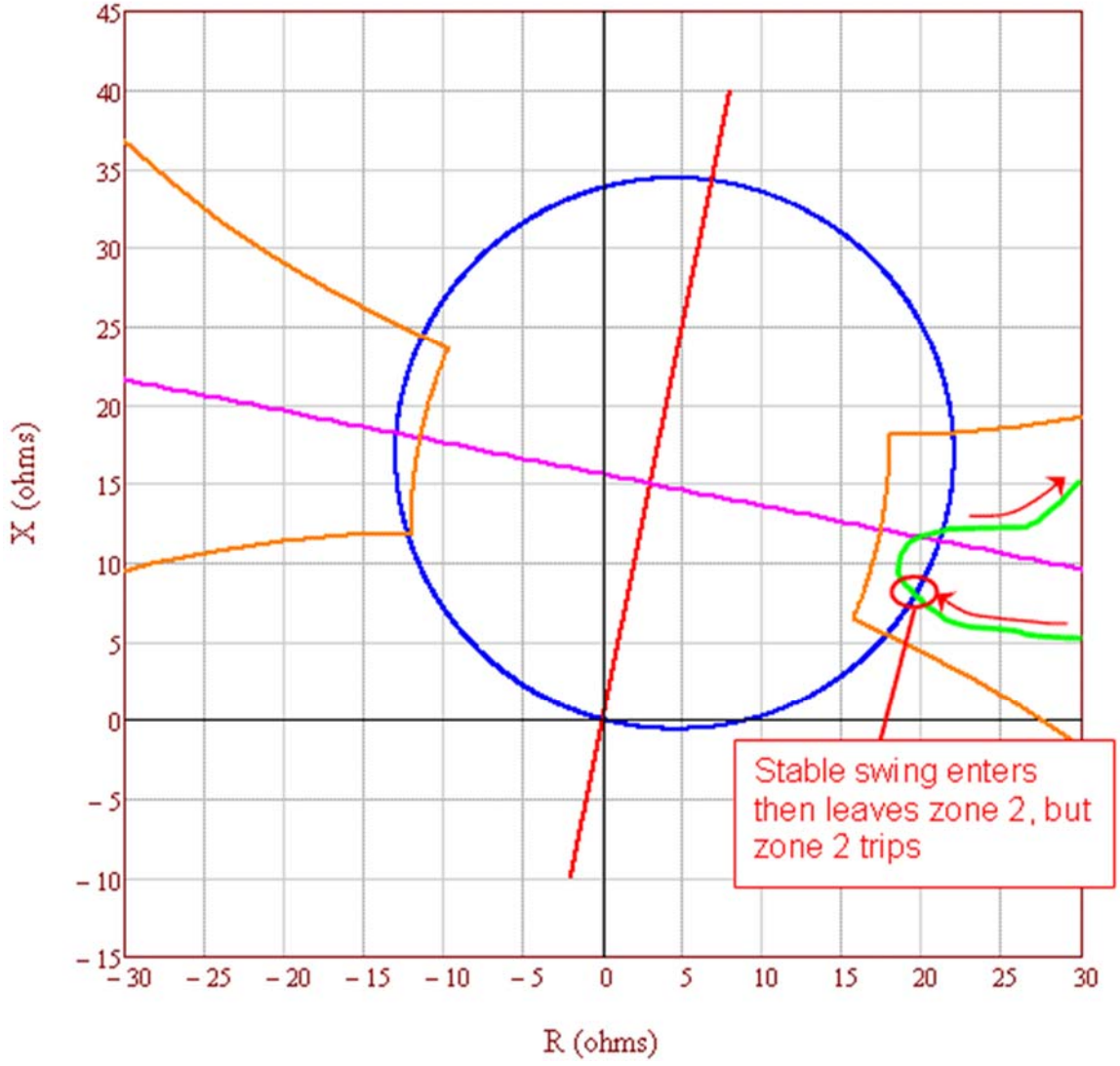


Figure 27: Relays on circuit breakers 2 and 4 were not addressed to meet the PRC-026-1 – Attachment B criteria following the previous unstable power swing event.

If the relays on circuit breakers 2 and 4 were not addressed under the Requirements for the previous unstable power swing condition, the relays would trip in response to the stable power swing, which would result in unnecessary system separation, load shedding, and possibly cascading or blackout.

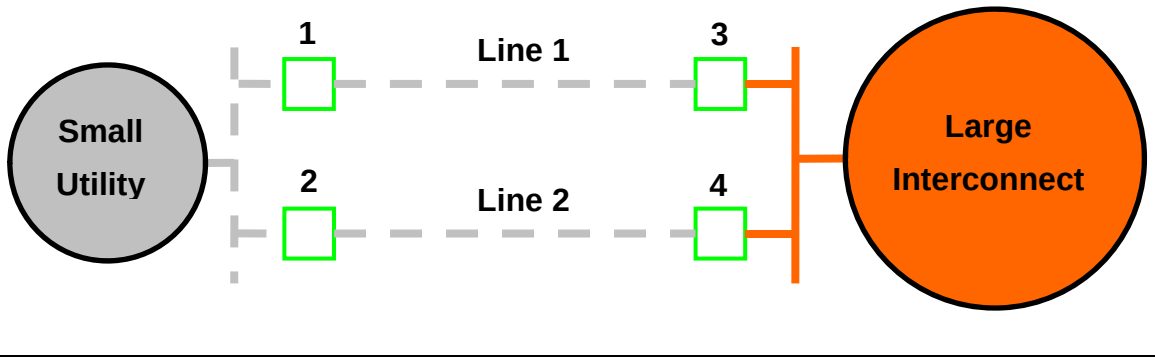


Figure 28: Possible blackout of the small utility.

If the relays that tripped in response to the previous unstable power swing condition in Figure 24 were addressed under the Requirements to meet PRC-026-1 - Attachment B criteria, the unnecessary tripping of the relays for the stable power swing shown in Figure 28 would have been averted, and the possible blackout of the small utility would have been avoided.

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 Planning Coordinator has a wide-area view and is in the position to identify generator, transformer, and transmission line BES Elements which meet the criteria, if any. The criteria-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document *Protection System Response to Power Swings*, August 2013 ("PSRPS Report"),[30] which recommends a focused approach to determine an at-risk BES Element. See the Guidelines and Technical Basis for a detailed discussion of the criteria.

Rationale for R2

The Generator Owner and Transmission Owner are in a position to determine whether their load-responsive protective relays meet the PRC-026-1 – Attachment B criteria. Generator, transformer, and transmission line BES Elements are identified by the Planning Coordinator in Requirement R1 and by the Generator Owner and Transmission Owner following an actual event where the Generator Owner and Transmission Owner became aware (i.e., through an event analysis or

[30] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

Protection System review) tripping was due to a stable or unstable power swing. A period of 12 calendar months allows sufficient time for the entity to conduct the evaluation.

Rationale for R3

To meet the reliability purpose of the standard, a CAP is necessary to ensure the entity's Protection System meets the PRC-026-1 – Attachment B criteria (1st bullet) so that protective relays are expected to not trip in response to stable power swings. A CAP may also be developed to modify the Protection System for exclusion under PRC-026-1 – Attachment A (2nd bullet). Such an exclusion will allow the Protection System to be exempt from the Requirement for future events. The phrase, "…while maintaining dependable fault detection and dependable out-of-step tripping…" in Requirement R3 describes that the entity is to comply with this standard, while achieving their desired protection goals. Refer to the Guidelines and Technical Basis, Introduction, for more information.

Rationale for R4

Implementation of the CAP must accomplish all identified actions to be complete to achieve the desired reliability goal. During the course of implementing a CAP, updates may be necessary for a variety of reasons such as new information, scheduling conflicts, or resource issues. Documenting CAP changes and completion of activities provides measurable progress and confirmation of completion.

Rationale for Attachment B (Criterion A)

The PRC-026-1 – Attachment B, Criterion A provides a basis for determining if the relays are expected to not trip for a stable power swing having a system separation angle of up to 120 degrees with the sending-end and receiving-end voltages varying from 0.7 to 1.0 per unit (See Guidelines and Technical Basis).

Standard Development Timeline

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

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

Anticipated Actions	Date
45-day formal comment period with initial ballot	June 2018 – July 2018
10-day final ballot	September 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** **Relay Performance During Stable Power Swings**

2. **Number:** **PRC-026-2~~1~~**

3. **Purpose:** To ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Generator Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.1.2 Planning Coordinator.

   4.1.3 Transmission Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.2. Facilities: The following Elements that are part of the Bulk Electric System (BES):

   4.2.1 Generators.

   4.2.2 Transformers.

   4.2.3 Transmission lines.

5. **Background:**

   This is the third phase of a three-phased standard development project that focused on developing this new Reliability Standard to address protective relay operations due to stable power swings. The March 18, 2010, Federal Energy Regulatory Commission (FERC) Order No. 733 approved Reliability Standard PRC-023-1 – Transmission Relay Loadability. In that Order, FERC directed NERC to address three areas of relay loadability that include modifications to the approved PRC-023-1, development of a new Reliability Standard to address generator protective relay loadability, and a new Reliability Standard to address the operation of protective relays due to stable power swings. This project's SAR addresses these directives with a three-phased approach to standard development.

   Phase 1 focused on making the specific modifications from FERC Order No. 733 to PRC-023-1. Reliability Standard PRC-023-2, which incorporated these modifications, became mandatory on July 1, 2012.

   Phase 2 focused on developing a new Reliability Standard, PRC-025-1 – Generator Relay Loadability, to address generator protective relay loadability. PRC-025-1 became mandatory on October 1, 2014, along with PRC-023-3, which was modified to harmonize PRC-023-2 with PRC-025-1.

   Phase 3 focuses on preventing protective relays from tripping unnecessarily due to stable power swings by requiring identification of Elements on which a stable or unstable power

swing may affect Protection System operation, assessment of the security of load-responsive protective relays to tripping in response to only a stable power swing, and implementation of Corrective Action Plans (CAP), where necessary. Phase 3 improves security of load-responsive protective relays for stable power swings so they are expected to not trip in response to stable power swings during non-Fault conditions while maintaining dependable fault detection and dependable out-of-step tripping.

6. Effective Dates:

Requirement R1

First day of the first full calendar year that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirements R2, R3, and R4

First day of the first full calendar year that is 36 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 36 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Planning Coordinator shall, at least once each calendar year, provide notification of each generator, transformer, and transmission line BES Element in its area that meets one or more of the following criteria, if any, to the respective Generator Owner and Transmission Owner: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

Criteria:

1. Generator(s) where an angular stability constraint exists that is addressed by a limiting the output of a generatorSystem Operating Limit (SOL) or a Remedial Action Scheme (RAS), and those Elements terminating at the Transmission station associated with the generator(s).
2. An Elements associated with that is monitored as part of an SOL identified by the Planning Coordinator's methodology[1] based on an angular instability identified in Planning Assessmentsconstraint.
3. An Element that forms the boundary of an island in the most recent underfrequency load shedding (UFLS) design assessment based on application of the Planning Coordinator's criteria for identifying islands, only if the island is formed by tripping the Element due to angular instability.
4. An Element identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[2] power swing during a simulated disturbance.

M1. Each Planning Coordinator shall have dated evidence that demonstrates notification of the generator, transformer, and transmission line BES Element(s) that meet one or more of the criteria in Requirement R1, if any, to the respective Generator Owner and Transmission Owner. Evidence may include, but is not limited to, the following documentation: emails, facsimiles, records, reports, transmittals, lists, or spreadsheets.

[1] NERC Reliability Standard FAC-014-2 – Establish and Communicate System Operating Limits, Requirement R3.

[2] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

R2. Each Generator Owner and Transmission Owner shall: [Violation Risk Factor: High] [Time Horizon: Operations Planning]

2.1 Within 12 full calendar months of notification of a BES Element pursuant to Requirement R1, determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B where an evaluation of that Element's load-responsive protective relay(s) based on PRC-026-1 – Attachment B criteria has not been performed in the last five calendar years.

2.2 Within 12 full calendar months of becoming aware[3] of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable[4] power swing due to the operation of its protective relay(s), determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B.

M2. Each Generator Owner and Transmission Owner shall have dated evidence that demonstrates the evaluation was performed according to Requirement R2. Evidence may include, but is not limited to, the following documentation: apparent impedance characteristic plots, email, design drawings, facsimiles, R-X plots, software output, records, reports, transmittals, lists, settings sheets, or spreadsheets.

R3. Each Generator Owner and Transmission Owner shall, within six full calendar months of determining a load-responsive protective relay does not meet the PRC-026-1 – Attachment B criteria pursuant to Requirement R2, develop a Corrective Action Plan (CAP) to meet one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- The Protection System meets the PRC-026-1 – Attachment B criteria, while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element); or
- The Protection System is excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element).

M3. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates the development of a CAP in accordance with Requirement R3. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

R4. Each Generator Owner and Transmission Owner shall implement each CAP developed pursuant to Requirement R3 and update each CAP if actions or timetables change until all actions are complete. *[Violation Risk Factor: Medium][Time Horizon: Long-Term Planning]*

M4. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates implementation of each CAP according to Requirement R4, including updates to the CAP when actions or timetables change. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

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 Generator Owner, Planning Coordinator, and Transmission Owner 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 Planning Coordinator shall retain evidence of Requirement R1 for a minimum of one calendar year following the completion of the Requirement.
- The Generator Owner and Transmission Owner shall retain evidence of Requirement R2 evaluation for a minimum of 12 calendar months following completion of each evaluation where a CAP is not developed.
- The Generator Owner and Transmission Owner shall retain evidence of Requirements R2, R3, and R4 for a minimum of 12 calendar months following completion of each CAP.

If a Generator Owner, Planning Coordinator, or Transmission Owner 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.

---

[3] Some examples of the ways an entity may become aware of a power swing are provided in the Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing."

[4] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure; "Compliance Monitoring and Assessment Processes" 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.

Table of Compliance Elements

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was less than or equal to 30 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 90 calendar days late. OR The Planning Coordinator failed to provide notification of the BES Element(s) in accordance with Requirement R1.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	High	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was less than or equal to 30 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 90 calendar days late. OR The Generator Owner or Transmission Owner failed to evaluate its load-responsive protective relay(s) in accordance with Requirement R2.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Long-term Planning	Medium	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than six calendar months and less than or equal to seven calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than seven calendar months and less than or equal to eight calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than eight calendar months and less than or equal to nine calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than nine calendar months. OR The Generator Owner or Transmission Owner failed to develop a CAP in accordance with Requirement R3.
R4	Long-term Planning	Medium	The Generator Owner or Transmission Owner implemented a Corrective Action Plan (CAP), but failed to update a CAP when actions or timetables changed, in accordance with Requirement R4.	N/A	N/A	The Generator Owner or Transmission Owner failed to implement a Corrective Action Plan (CAP) in accordance with Requirement R4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Applied Protective Relaying, Westinghouse Electric Corporation, 1979.

Burdy, John, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

IEEE Power System Relaying Committee WG D6, *Power Swing and Out-of-Step Considerations on Transmission Lines*, July 2005: http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Kimbark Edward Wilson, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

Kundur, Prabha, *Power System Stability and Control*, 1994, Palo Alto: EPRI, McGraw Hill, Inc.

NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf.

Reimert, Donald, *Protective Relaying for Power Generation Systems*, 2006, Boca Raton: CRC Press.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by NERC Board of Trustees	New
1	March 17, 2016	FERC Order issued approving PRC-026-1. Docket No. RM15-8-000.	

PRC-026-1 – Attachment A

This standard applies to any protective functions which could trip instantaneously or with a time delay of less than 15 cycles on load current (i.e., "load-responsive") including, but not limited to:

- Phase distance
- Phase overcurrent
- Out-of-step tripping
- Loss-of-field

The following protection functions are excluded from Requirements of this standard:

- Relay elements supervised by power swing blocking
- Relay elements that are only enabled when other relays or associated systems fail. For example:
    - Overcurrent elements that are only enabled during loss of potential conditions.
    - Relay elements that are only enabled during a loss of communications
- Thermal emulation relays which are used in conjunction with dynamic Facility Ratings
- Relay elements associated with direct current (dc) lines
- Relay elements associated with dc converter transformers
- Phase fault detector relay elements employed to supervise other load-responsive phase distance elements (i.e., in order to prevent false operation in the event of a loss of potential)
- Relay elements associated with switch-onto-fault schemes
- Reverse power relay on the generator
- Generator relay elements that are armed only when the generator is disconnected from the system, (e.g., non-directional overcurrent elements used in conjunction with inadvertent energization schemes, and open breaker flashover schemes)
- Current differential relay, pilot wire relay, and phase comparison relay
- Voltage-restrained or voltage-controlled overcurrent relays

PRC-026-1 – Attachment B

Criterion A:

An impedance-based relay used for tripping is expected to not trip for a stable power swing, when the relay characteristic is completely contained within the unstable power swing region.[5] The unstable power swing region is formed by the union of three shapes in the impedance (R-X) plane; (1) a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7; (2) an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43; (3) a lens that connects the endpoints of the total system impedance (with the parallel transfer impedance removed) bounded by varying the sending-end and receiving-end voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance where:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.

[5] Guidelines and Technical Basis, Figures 1 and 2.

PRC-026-1 – Attachment B

Criterion B:

The pickup of an overcurrent relay element used for tripping, that is above the calculated current value (with the parallel transfer impedance removed) for the conditions below:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.
4. Both the sending-end and receiving-end voltages at 1.05 per unit.

Guidelines and Technical Basis

Introduction

The NERC System Protection and Control Subcommittee technical document, *Protection System Response to Power Swings*, August 2013,[6] ("PSRPS Report" or "report") was specifically prepared to support the development of this NERC Reliability Standard. The report provided a historical perspective on power swings as early as 1965 up through the approval of the report by the NERC Planning Committee. The report also addresses reliability issues regarding trade-offs between security and dependability of Protection Systems, considerations for this NERC Reliability Standard, and a collection of technical information about power swing characteristics and varying issues with practical applications and approaches to power swings. Of these topics, the report suggests an approach for this NERC Reliability Standard ("standard" or "PRC-026-1") which is consistent with addressing three regulatory directives in the FERC Order No. 733. The first directive concerns the need for "…protective relay systems that differentiate between faults and stable power swings and, when necessary, phases out protective relay systems that cannot meet this requirement."[7] Second, is "…to develop a Reliability Standard addressing undesirable relay operation due to stable power swings."[8] The third directive "…to consider "islanding" strategies that achieve the fundamental performance for all islands in developing the new Reliability Standard addressing stable power swings"[9] was considered during development of the standard.

The development of this standard implements the majority of the approaches suggested by the report. However, it is noted that the Reliability Coordinator and Transmission Planner have not been included in the standard's Applicability section (as suggested by the PSRPS Report). This is so that a single entity, the Planning Coordinator, may be the single source for identifying Elements according to Requirement R1. A single source will insure that multiple entities will not identify Elements in duplicate, nor will one entity fail to provide an Element because it believes the Element is being provided by another entity. The Planning Coordinator has, or has access to, the wide-area model and can correctly identify the Elements that may be susceptible to a stable or unstable power swing. Additionally, not including the Reliability Coordinator and Transmission Planner is consistent with the applicability of other relay loadability NERC Reliability Standards (e.g., PRC-023 and PRC-025). It is also consistent with the NERC Functional Model.

The phrase, "while maintaining dependable fault detection and dependable out-of-step tripping" in Requirement R3, describes that the Generator Owner and Transmission Owner are to comply with this standard while achieving its desired protection goals. Load-responsive protective relays, as addressed within this standard, may be intended to provide a variety of backup protection functions, both within the generating unit or generating plant and on the transmission system, and

---

[6] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

[7] Transmission Relay Loadability Reliability Standard, Order No. 733, P.150 FERC ¶ 61,221 (2010).

[8] Ibid. P.153.

[9] Ibid. P.162.

this standard is not intended to result in the loss of these protection functions. Instead, the Generator Owner and Transmission Owner must consider both the Requirements within this standard and its desired protection goals and perform modifications to its protective relays or protection philosophies as necessary to achieve both.

Power Swings

The IEEE Power System Relaying Committee WG D6 developed a technical document called *Power Swing and Out-of-Step Considerations on Transmission Lines* (July 2005) that provides background on power swings. The following are general definitions from that document:[10]

> Power Swing: a variation in three phase power flow which occurs when the generator rotor angles are advancing or retarding relative to each other in response to changes in load magnitude and direction, line switching, loss of generation, faults, and other system disturbances.
>
> Pole Slip: a condition whereby a generator, or group of generators, terminal voltage angles (or phases) go past 180 degrees with respect to the rest of the connected power system.
>
> Stable Power Swing: a power swing is considered stable if the generators do not slip poles and the system reaches a new state of equilibrium, i.e. an acceptable operating condition.
>
> Unstable Power Swing: a power swing that will result in a generator or group of generators experiencing pole slipping for which some corrective action must be taken.
>
> Out-of-Step Condition: Same as an unstable power swing.
>
> Electrical System Center or Voltage Zero: it is the point or points in the system where the voltage becomes zero during an unstable power swing.

Burden to Entities

The PSRPS Report provides a technical basis and approach for focusing on Protection Systems, which are susceptible to power swings, while achieving the purpose of the standard. The approach reduces the number of relays to which the PRC-026-1 Requirements would apply by first identifying the BES Element(s) on which load-responsive protective relays must be evaluated. The first step uses criteria to identify the Elements on which a Protection System is expected to be challenged by power swings. Of those Elements, the second step is to evaluate each load-responsive protective relay that is applied on each identified Element. Rather than requiring the Planning Coordinator or Transmission Planner to perform simulations to obtain information for each identified Element, the Generator Owner and Transmission Owner will reduce the need for simulation by comparing the load-responsive protective relay characteristic to specific criteria in PRC-026-1 – Attachment B.

[10] http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Applicability

The standard is applicable to the Generator Owner, Planning Coordinator, and Transmission Owner entities. More specifically, the Generator Owner and Transmission Owner entities are applicable when applying load-responsive protective relays at the terminals of the applicable BES Elements. The standard is applicable to the following BES Elements: generators, transformers, and transmission lines. The Distribution Provider was considered for inclusion in the standard; however, it is not subject to the standard because this entity, by functional registration, would not own generators, transmission lines, or transformers other than load serving.

Load-responsive protective relays include any protective functions which could trip with or without time delay, on load current.

Requirement R1

The Planning Coordinator has a wide-area view and is in the position to identify what, if any, Elements meet the criteria. The criterion-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document, *Protection System Response to Power Swings (*August 2013),[11] which recommends a focused approach to determine an at-risk Element. Identification of Elements comes from the annual Planning Assessments pursuant to the transmission planning (i.e., "TPL") and other NERC Reliability Standards (e.g., PRC-006), and the standard is not requiring any other assessments to be performed by the Planning Coordinator. The required notification on a calendar year basis to the respective Generator Owner and Transmission Owner is sufficient because it is expected that the Planning Coordinator will make its notifications following the completion of its annual Planning Assessments. The Planning Coordinator will continue to provide notification of Elements on a calendar year basis even if a study is performed less frequently (e.g., PRC-006 – Automatic Underfrequency Load Shedding, which is five years) and has not changed. It is possible that a Planning Coordinator could utilize studies from a prior year in determining the necessary notifications pursuant to Requirement R1.

Criterion 1

The first criterion involves generator(s) where an angular stability constraint exists that is addressed by limiting the output of a generator~~a System Operating Limit (SOL)~~ or a Remedial Action Scheme (RAS) and those Elements terminating at the Transmission station associated with the generator(s). For example, a scheme to remove generation for specific conditions is implemented for a four-unit generating plant (1,100 MW). Two of the units are 500 MW each; one is connected to the 345 kV system and one is connected to the 230 kV system. The Transmission Owner has two 230 kV transmission lines and one 345 kV transmission line all terminating at the generating facility as well as a 345/230 kV autotransformer. The remaining 100 MW consists of two 50 MW combustion turbine (CT) units connected to four 66 kV transmission lines. The 66 kV transmission lines are not electrically joined to the 345 kV and 230 kV transmission lines at the plant site and are not subject to ~~the operating limit~~ any generating output limitation or RAS. A

[11] http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

stability constraint limits the output of the portion of the plant affected by the RAS to 700 MW for an outage of the 345 kV transmission line. The RAS trips one of the 500 MW units to maintain stability for a loss of the 345 kV transmission line when the total output from both 500 MW units is above 700 MW. For this example, both 500 MW generating units and the associated generator step-up (GSU) transformers would be identified as Elements meeting this criterion. The 345/230 kV autotransformer, the 345 kV transmission line, and the two 230 kV transmission lines would also be identified as Elements meeting this criterion. The 50 MW combustion turbines and 66 kV transmission lines would not be identified pursuant to Criterion 1 because these Elements are not subject to ~~an operating limit~~ any generating output limitation or RAS and do not terminate at the Transmission station associated with the generators that are subject to any generating output limitation~~the SOL~~ or RAS.

Criterion 2

The second criterion involves Elements associated with angular instability identified in the Planning Assessments~~that are monitored as a part of an established System Operating Limit (SOL) based on an angular stability limit regardless of the outage conditions that result in the enforcement of the SOL~~. For example, if Planning Assessments have identified that an angular instability could limit transfer capability on two long parallel 500 kV transmission lines ~~have a combined SOL of~~ to a maximum of 1,200 MW, and this limitation is based on angular instability resulting from a fault and subsequent loss of one of the two lines, then both lines would be identified as Elements meeting the criterion.

Criterion 3

The third criterion involves Elements that form the boundary of an island within an underfrequency load shedding (UFLS) design assessment. The criterion applies to islands identified based on application of the Planning Coordinator's criteria for identifying islands, where the island is formed by tripping the Elements based on angular instability. The criterion applies if the angular instability is modeled in the UFLS design assessment, or if the boundary is identified "off-line" (i.e., the Elements are selected based on angular instability considerations, but the Elements are tripped in the UFLS design assessment without modeling the initiating angular instability). In cases where an out-of-step condition is detected and tripping is initiated at an alternate location, the criterion applies to the Element on which the power swing is detected. The criterion does not apply to islands identified based on other considerations that do not involve angular instability, such as excessive loading, Planning Coordinator area boundary tie lines, or Balancing Authority boundary tie lines.

Criterion 4

The fourth criterion involves Elements identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[12] power swing during a simulated

[12] Refer to the "Justification for Including Unstable Power Swings in the Requirements" section.

disturbance. The intent is for the Planning Coordinator to include any Element(s) where relay tripping was observed during simulations performed for the most recent annual Planning Assessment associated with the transmission planning TPL-001-4 Reliability Standard. Note that relay tripping must be assessed within those annual Planning Assessments per TPL-001-4, R4, Part 4.3.1.3, which indicates that analysis shall include the "Tripping of Transmission lines and transformers where transient swings cause Protection System operation based on generic or actual relay models." Identifying such Elements according to Criterion 4 and notifying the respective Generator Owner and Transmission Owner will require that the owners of any load-responsive protective relay applied at the terminals of the identified Element evaluate the relay's susceptibility to tripping in response to a stable power swing.

Planning Coordinators have the discretion to determine whether the observed tripping for a power swing in its Planning Assessments occurs for valid contingencies and system conditions. The Planning Coordinator will address tripping that is observed in transient analyses on an individual basis; therefore, the Planning Coordinator is responsible for identifying the Elements based only on simulation results that are determined to be valid.

Due to the nature of how a Planning Assessment is performed, there may be cases where a previously-identified Element is not identified in the most recent annual Planning Assessment. If so, this is acceptable because the Generator Owner and Transmission Owner would have taken action upon the initial notification of the previously identified Element. When an Element is not identified in later Planning Assessments, the risk of load-responsive protective relays tripping in response to a stable power swing during non-Fault conditions would have already been assessed under Requirement R2 and mitigated according to Requirements R3 and R4 where the relays did not meet the PRC-026-1 – Attachment B criteria. According to Requirement R2, the Generator Owner and Transmission Owner are only required to re-evaluate each load-responsive protective relay for an identified Element where the evaluation has not been performed in the last five calendar years.

Although Requirement R1 requires the Planning Coordinator to notify the respective Generator Owner and Transmission Owner of any Elements meeting one or more of the four criteria, it does not preclude the Planning Coordinator from providing additional information, such as apparent impedance characteristics, in advance or upon request, that may be useful in evaluating protective relays. Generator Owners and Transmission Owners are able to complete protective relay evaluations and perform the required actions without additional information. The standard does not include any requirement for the entities to provide information that is already being shared or exchanged between entities for operating needs. While a Requirement has not been included for the exchange of information, entities should recognize that relay performance needs to be measured against the most current information.

Requirement R2

Requirement R2 requires the Generator Owner and Transmission Owner to evaluate its load-responsive protective relays to ensure that they are expected to not trip in response to stable power swings.

The PRC-026-1 – Attachment A lists the applicable load-responsive relays that must be evaluated which include phase distance, phase overcurrent, out-of-step tripping, and loss-of-field relay functions. Phase distance relays could include, but are not limited to, the following:

- Zone elements with instantaneous tripping or intentional time delays of less than 15 cycles
- Phase distance elements used in high-speed communication-aided tripping schemes including:
  - Directional Comparison Blocking (DCB) schemes
  - Directional Comparison Un-Blocking (DCUB) schemes
  - Permissive Overreach Transfer Trip (POTT) schemes
  - Permissive Underreach Transfer Trip (PUTT) schemes

A method is provided within the standard to support consistent evaluation by Generator Owners and Transmission Owners based on specified conditions. Once a Generator Owner or Transmission Owner is notified of Elements pursuant to Requirement R1, it has 12 full calendar months to determine if each Element's load-responsive protective relays meet the PRC-026-1 – Attachment B criteria, if the determination has not been performed in the last five calendar years. Additionally, each Generator Owner and Transmission Owner, that becomes aware of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable power swing due to the operation of its protective relays pursuant to Requirement R2, Part 2.2, must perform the same PRC-026-1 – Attachment B criteria determination within 12 full calendar months.

Becoming Aware of an Element That Tripped in Response to a Power Swing

Part 2.2 in Requirement R2 is intended to initiate action by the Generator Owner and Transmission Owner when there is a known stable or unstable power swing and it resulted in the entity's Element tripping. The criterion starts with becoming aware of the event (i.e., power swing) and then any connection with the entity's Element tripping. By doing so, the focus is removed from the entity having to demonstrate that it made a determination whether a power swing was present for every Element trip. The basis for structuring the criterion in this manner is driven by the available ways that a Generator Owner and Transmission Owner could become aware of an Element that tripped in response to a stable or unstable power swing due to the operation of its protective relay(s).

Element trips caused by stable or unstable power swings, though infrequent, would be more common in a larger event. The identification of power swings will be revealed during an analysis of the event. Event analysis where an entity may become aware of a stable or unstable power swing could include internal analysis conducted by the entity, the entity's Protection System review following a trip, or a larger scale analysis by other entities. Event analysis could include involvement by the entity's Regional Entity, and in some cases NERC.

Information Common to Both Generation and Transmission Elements

The PRC-026-1 – Attachment A lists the load-responsive protective relays that are subject to this standard. Generator Owners and Transmission Owners may own load-responsive protective relays (e.g., distance relays) that directly affect generation or transmission BES Elements and will require analysis as a result of Elements being identified by the Planning Coordinator in Requirement R1

or the Generator Owner or Transmission Owner in Requirement R2. For example, distance relays owned by the Transmission Owner may be installed at the high-voltage side of the generator step-up (GSU) transformer (directional toward the generator) providing backup to generation protection. Generator Owners may have distance relays applied to backup transmission protection or backup protection to the GSU transformer. The Generator Owner may have relays installed at the generator terminals or the high-voltage side of the GSU transformer.

Exclusion of Time Based Load-Responsive Protective Relays

The purpose of the standard is "[t]o ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions." Load-responsive, high-speed tripping protective relays pose the highest risk of operating during a power swing. Because of this, high-speed tripping protective relays and relays with a time delay of less than 15 cycles are included in the standard; whereas other relays (i.e., Zones 2 and 3) with a time delay of 15 cycles or greater are excluded. The time delay used for exclusion on some load-responsive protective relays is based on the maximum expected time that load-responsive protective relays would be exposed to a stable power swing with a slow slip rate frequency.

In order to establish a time delay that distinguishes a high-risk load-responsive protective relay from one that has a time delay for tripping (lower-risk), a sample of swing rates were calculated based on a stable power swing entering and leaving the impedance characteristic as shown in Table 1. For a relay impedance characteristic that has a power swing entering and leaving, beginning at 90 degrees with a termination at 120 degrees before exiting the zone, the zone timer must be greater than the calculated time the stable power swing is inside the relay's operating zone to not trip in response to the stable power swing.

Eq. (1) $$Zone\ timer > 2 \times \left(\frac{(120° - Angle\ of\ entry\ into\ the\ relay\ characteristic) \times 60}{(360 \times Slip\ Rate)}\right)$$

Table 1: Swing Rates

Zone Timer (Cycles)	Slip Rate (Hz)
10	1.00
15	0.67
20	0.50
30	0.33

With a minimum zone timer of 15 cycles, the corresponding slip rate of the system is 0.67 Hz. This represents an approximation of a slow slip rate during a system Disturbance. Longer time delays allow for slower slip rates.

Application to Transmission Elements

Criterion A in PRC-026-1 – Attachment B describes an unstable power swing region that is formed by the union of three shapes in the impedance (R-X) plane. The first shape is a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7 (i.e., E_S / E_R = 0.7 / 1.0 = 0.7). The second shape is an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43 (i.e., E_S / E_R = 1.0 / 0.7 = 1.43). The third shape is a lens that connects the endpoints of the total system impedance together by varying the sending-end and receiving-end system voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance (with the parallel transfer impedance removed—see Figures 1 through 5). The total system impedance is derived from a two-bus equivalent network and is determined by summing the sending-end source impedance, the line impedance (excluding the Thévenin equivalent transfer impedance), and the receiving-end source impedance as shown in Figures 6 and 7. Establishing the total system impedance provides a conservative condition that will maximize the security of the relay against various system conditions. The smallest total system impedance represents a condition where the size of the lens characteristic in the R-X plane is smallest and is a conservative operating point from the standpoint of ensuring a load-responsive protective relay is expected to not trip given a predetermined angular displacement between the sending-end and receiving-end voltages. The smallest total system impedance results when all generation is in service and all transmission BES Elements are modeled in their "normal" system configuration (PRC-026-1 – Attachment B, Criterion A). The parallel transfer impedance is removed to represent a likely condition where parallel Elements may be lost during the disturbance, and the loss of these Elements magnifies the sensitivity of the load-responsive relays on the parallel line by removing the "infeed effect" (i.e., the apparent impedance sensed by the relay is decreased as a result of the loss of the transfer impedance, thus making the relay more likely to trip for a stable power swing—See Figures 13 and 14).

The sending-end and receiving-end source voltages are varied from 0.7 to 1.0 per unit to form the lower and upper loss-of-synchronism circles. The ratio of these two voltages is used in the calculation of the loss-of-synchronism circles, and result in a ratio range from 0.7 to 1.43.

Eq. (2) $$\frac{E_S}{E_R} = \frac{0.7}{1.0} = 0.7$$

Eq. (3): $$\frac{E_S}{E_R} = \frac{1.0}{0.7} = 1.43$$

The internal generator voltage during severe power swings or transmission system fault conditions will be greater than zero due to voltage regulator support. The voltage ratio of 0.7 to 1.43 is chosen to be more conservative than the PRC-023[13] and PRC-025[14] NERC Reliability Standards where a lower bound voltage of 0.85 per unit voltage is used. A ±15% internal generator voltage range was chosen as a conservative voltage range for calculation of the voltage ratio used to calculate the loss-of-synchronism circles. For example, the voltage ratio using these voltages would result in a ratio range from 0.739 to 1.353.

[13] Transmission Relay Loadability

[14] Generator Relay Loadability

Eq. (4) $$\frac{E_S}{E_R} = \frac{0.85}{1.15} = 0.739$$ Eq. (5): $$\frac{E_S}{E_R} = \frac{1.15}{0.85} = 1.353$$

The lower ratio is rounded down to 0.7 to be more conservative, allowing a voltage range of 0.7 to 1.0 per unit to be used for the calculation of the loss-of-synchronism circles.[15]

When the parallel transfer impedance is included in the model, the division of current through the parallel transfer impedance path results in actual measured relay impedances that are larger than those measured when the parallel transfer impedance is removed (i.e., infeed effect), which would make it more likely for an impedance relay element to be completely contained within the unstable power swing region as shown in Figure 11. If the transfer impedance is included in the evaluation, a distance relay element could be deemed as meeting PRC-026-1 – Attachment B criteria and, in fact would be secure, assuming all Elements were in their normal state. In this case, the distance relay element could trip in response to a stable power swing during an actual event if the system was weakened (i.e., a higher transfer impedance) by the loss of a subset of lines that make up the parallel transfer impedance as shown in Figure 10. This could happen because the subset of lines that make up the parallel transfer impedance tripped on unstable swings, contained the initiating fault, and/or were lost due to operation of breaker failure or remote back-up protection schemes.

Table 10 shows the percent size increase of the lens shape as seen by the relay under evaluation when the parallel transfer impedance is included. The parallel transfer impedance has minimal effect on the apparent size of the lens shape as long as the parallel transfer impedance is at least 10 multiples of the parallel line impedance (less than 5% lens shape expansion), therefore, its removal has minimal impact, but results in a slightly more conservative, smaller lens shape. Parallel transfer impedances of 5 multiples of the parallel line impedance or less result in an apparent lens shape size of 10% or greater as seen by the relay. If two parallel lines and a parallel transfer impedance tie the sending-end and receiving-end buses together, the total parallel transfer impedance will be one or less multiples of the parallel line impedance, resulting in an apparent lens shape size of 45% or greater. It is a realistic contingency that the parallel line could be out-of-service, leaving the parallel transfer impedance making up the rest of the system in parallel with the line impedance. Since it is not known exactly which lines making up the parallel transfer impedance will be out of service during a major system disturbance, it is most conservative to assume that all of them are out, leaving just the line under evaluation in service.

Either the saturated transient or sub-transient direct axis reactance may be used for machines in the evaluation because they are smaller than the un-saturated reactances. Since saturated sub-transient generator reactances are smaller than the transient or synchronous reactances, the use of sub-transient reactances will result in a smaller source impedance and a smaller unstable power swing region in the graphical analysis as shown in Figures 8 and 9. Because power swings occur in a time frame where generator transient reactances will be prevalent, it is acceptable to use saturated transient reactances instead of saturated sub-transient reactances. Because some short-

[15] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, Section 6 (The Cascade Stage of the Blackout), p. 94 under "Why the Generators Tripped Off," states, "Some generator undervoltage relays were set to trip at or above 90% voltage. However, a motor stalls out at about 70% voltage and a motor starter contactor drops out around 75%, so if there is a compelling need to protect the turbine from the system the under-voltage trigger point should be no higher than 80%."

circuit models may not include transient reactances, the use of sub-transient reactances is also acceptable because it produces more conservative results. For this reason, either value is acceptable when determining the system source impedances (PRC-026-1 – Attachment B, Criterion A and B, No. 3).

Saturated reactances are used in short-circuit programs that produce the system impedance mentioned above. Planning and stability software generally use un-saturated reactances. Generator models used in transient stability analyses recognize that the extent of the saturation effect depends upon both rotor (field) and stator currents. Accordingly, they derive the effective saturated parameters of the machine at each instant by internal calculation from the specified (constant) unsaturated values of machine reactances and the instantaneous internal flux level. The specific assumptions regarding which inductances are affected by saturation, and the relative effect of that saturation, are different for the various generator models used. Thus, unsaturated values of all machine reactances are used in setting up planning and stability software data, and the appropriate set of open-circuit magnetization curve data is provided for each machine.

Saturated reactance values are smaller than unsaturated reactance values and are used in short-circuit programs owned by the Generator and Transmission Owners. Because of this, saturated reactance values are to be used in the development of the system source impedances.

The source or system equivalent impedances can be obtained by a number of different methods using commercially available short-circuit calculation tools.[16] Most short-circuit tools have a network reduction feature that allows the user to select the local and remote terminal buses to retain. The first method reduces the system to one that contains two buses, an equivalent generator at each bus (representing the source impedances at the sending-end and receiving-end), and two parallel lines; one being the line impedance of the protected line with relays being analyzed, the other being the parallel transfer impedance representing all other combinations of lines that connect the two buses together as shown in Figure 6. Another conservative method is to open both ends of the line being evaluated, and apply a three-phase bolted fault at each bus to determine the Thévenin equivalent impedance at each bus. The source impedances are set equal to the Thévenin equivalent impedances and will be less than or equal to the actual source impedances calculated by the network reduction method. Either method can be used to develop the system source impedances at both ends.

The two bullets of PRC-026-1 – Attachment B, Criterion A, No. 1, identify the system separation angles used to identify the size of the power swing stability boundary for evaluating load-responsive protective relay impedance elements. The first bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates a system separation angle of at least 120 degrees that is held constant while varying the sending-end and receiving-end source voltages from 0.7 to 1.0 per unit, thus creating an unstable power swing region about the total system impedance in Figure 1. This unstable power swing region is compared to the tripping portion of the distance relay characteristic; that is, the portion that is not supervised by load encroachment, blinders, or some other form of supervision as shown in Figure 12 that restricts the distance element from tripping

[16] Demetrios A. Tziouvaras and Daqing Hou, Appendix in *Out-Of-Step Protection Fundamentals and Advancements,* April 17, 2014: https://www.selinc.com.

for heavy, balanced load conditions. If the tripping portion of the impedance characteristics are completely contained within the unstable power swing region, the relay impedance element meets Criterion A in PRC-026-1 – Attachment B. A system separation angle of 120 degrees was chosen for the evaluation because it is generally accepted in the industry that recovery for a swing beyond this angle is unlikely to occur.[17]

The second bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates impedance relay elements at a system separation angle of less than 120 degrees, similar to the first bullet described above. An angle less than 120 degrees may be used if a documented stability analysis demonstrates that the power swing becomes unstable at a system separation angle of less than 120 degrees.

The exclusion of relay elements supervised by Power Swing Blocking (PSB) in PRC-026-1 – Attachment A allows the Generator Owner or Transmission Owner to exclude protective relay elements if they are blocked from tripping by PSB relays. A PSB relay applied and set according to industry accepted practices prevent supervised load-responsive protective relays from tripping in response to power swings. Further, PSB relays are set to allow dependable tripping of supervised elements. The criteria in PRC-026-1 – Attachment B specifically applies to unsupervised elements that could trip for stable power swings. Therefore, load-responsive protective relay elements supervised by PSB can be excluded from the Requirements of this standard.

[17] "The critical angle for maintaining stability will vary depending on the contingency and the system condition at the time the contingency occurs; however, the likelihood of recovering from a swing that exceeds 120 degrees is marginal and 120 degrees is generally accepted as an appropriate basis for setting out-of-step protection. Given the importance of separating unstable systems, defining 120 degrees as the critical angle is appropriate to achieve a proper balance between dependable tripping for unstable power swings and secure operation for stable power swings." NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf), p. 28.

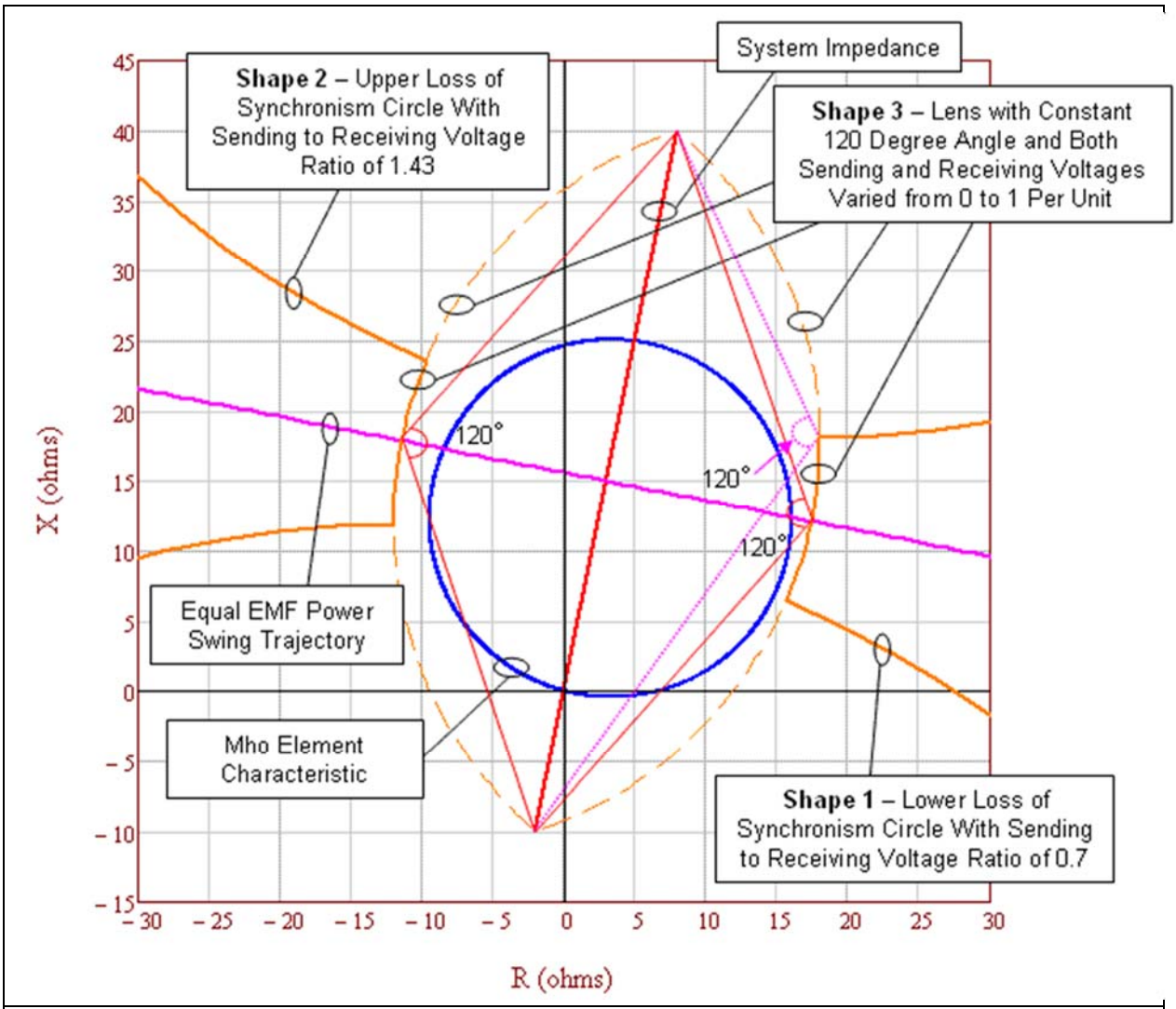


Figure 1: An enlarged graphic illustrating the unstable power swing region formed by the union of three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region (i.e., it does not intersect any portion of the unstable power swing region), therefore it meets PRC-026-1 – Attachment B, Criterion A, No. 1.

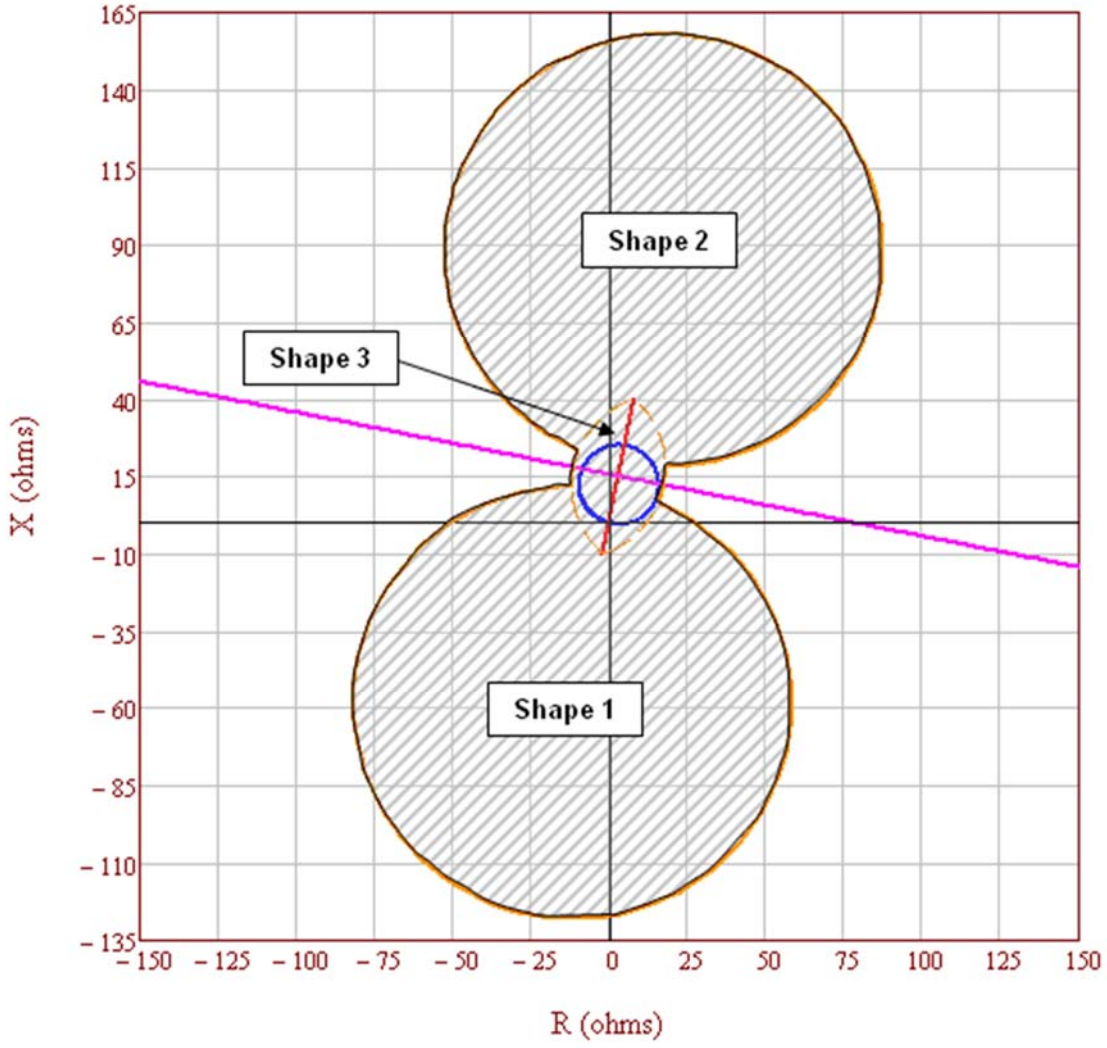


Figure 2: Full graphic of the unstable power swing region formed by the union of the three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region, therefore it meets PRC-26-1 – Attachment B, Criterion A, No.1.

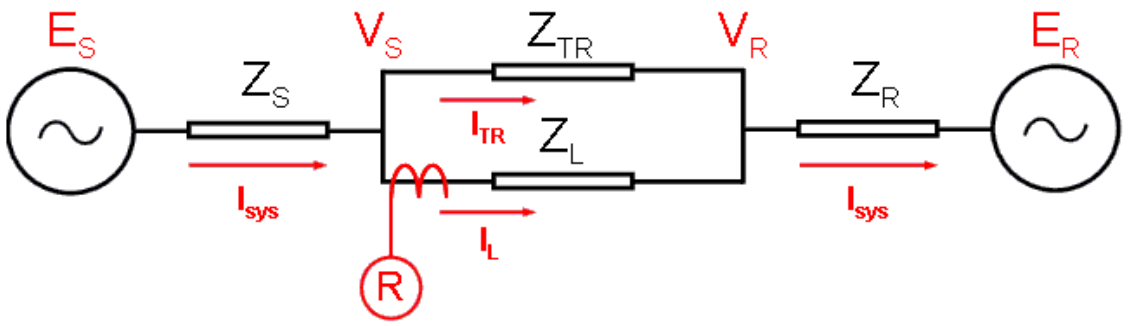


Figure 3: System impedances as seen by Relay R (voltage connections are not shown).

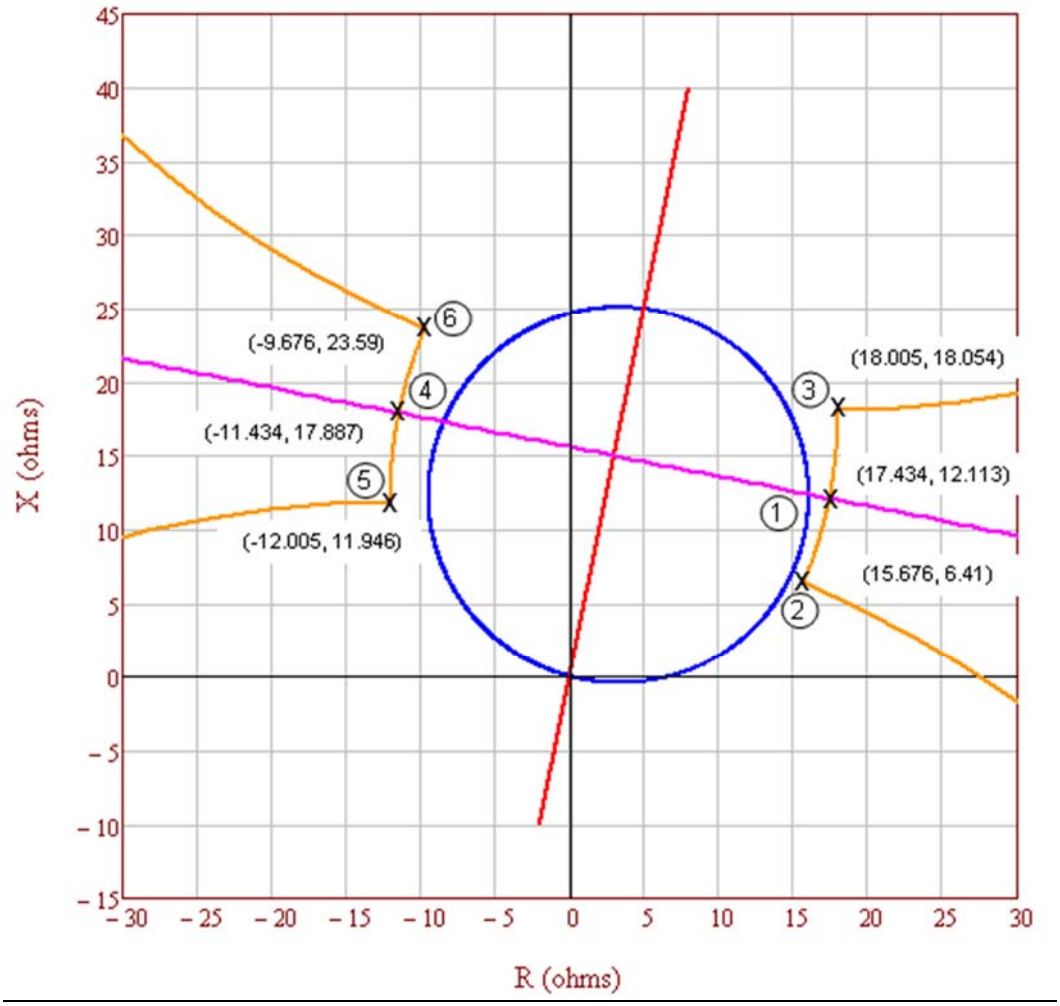


Figure 4: The defining unstable power swing region points where the lens shape intersects the lower and upper loss-of-synchronism circle shapes and where the lens intersects the equal EMF (electromotive force) power swing.

	Left Side Coordinates		Right Side Coordinates	
E_S / E_R Voltage Ratio	R	+ jX	R	+ jX
0.7	**-12.005**	**11.946**	**15.676**	**6.41**
0.72	-12.004	12.407	15.852	6.836
0.74	-11.996	12.857	16.018	7.255
0.76	-11.982	13.298	16.175	7.667
0.78	-11.961	13.729	16.321	8.073
0.8	-11.935	14.151	16.459	8.472
0.82	-11.903	14.563	16.589	8.865
0.84	-11.867	14.966	16.71	9.251
0.86	-11.826	15.361	16.824	9.631
0.88	-11.78	15.746	16.93	10.004
0.9	-11.731	16.123	17.03	10.371
0.92	-11.678	16.492	17.123	10.732
0.94	-11.621	16.852	17.209	11.086
0.96	-11.562	17.205	17.29	11.435
0.98	-11.499	17.55	17.364	11.777
1	**-11.434**	**17.887**	**17.434**	**12.113**
1.0286	-11.336	18.356	17.524	12.584
1.0572	-11.234	18.81	17.604	13.043
1.0858	-11.127	19.251	17.675	13.49
1.1144	-11.017	19.677	17.738	13.926
1.143	-10.904	20.091	17.792	14.351
1.1716	-10.788	20.491	17.84	14.766
1.2002	-10.67	20.88	17.88	15.17
1.2288	-10.55	21.256	17.914	15.564
1.2574	-10.428	21.621	17.942	15.948
1.286	-10.304	21.975	17.964	16.322
1.3146	-10.18	22.319	17.981	16.687
1.3432	-10.054	22.652	17.993	17.043
1.3718	-9.928	22.976	18.001	17.39
1.4004	-9.801	23.29	18.005	17.728
1.429	**-9.676**	**23.59**	**18.005**	**18.054**

Figure 5: Full table of 31 detailed lens shape point calculations. The bold highlighted rows correspond to the detailed calculations in Tables 2-7.

Table 2: Example Calculation (Lens Point 1)	
This example is for calculating the impedance the first point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 120 degrees. See Figures 3 and 4.	
Eq. (6)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$

Table 2: Example Calculation (Lens Point 1)			
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (7)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (8)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (9)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (10)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50\ )\Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (11)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		

Table 2: Example Calculation (Lens Point 1)	
	$I_L = 4{,}511\angle 71.3° \; A \times \frac{(4 + j20) \times 10^{10} \; \Omega}{(4 + j20) \; \Omega + (4 + j20) \times 10^{10} \; \Omega}$
	$I_L = 4{,}511\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (12)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10) \; \Omega \times 4{,}511\angle 71.3° \; A]$
	$V_S = 95{,}757\angle 106.1° \; V$
The impedance seen by the relay on Z_L.	
Eq. (13)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \; V}{4{,}511\angle 71.3° \; A}$
	$Z_{L-Relay} = 17.434 + j12.113 \; \Omega$

Table 3: Example Calculation (Lens Point 2)			
This example is for calculating the impedance second point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (14)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 120° \; V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 120° \; V$		
Eq. (15)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \; V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \; V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10 \; \Omega$	$Z_L = 4 + j20 \; \Omega$	$Z_R = 4 + j20 \; \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10} \; \Omega$		

Table 3: Example Calculation (Lens Point 2)	
Total impedance between the generators.	
Eq. (16)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (17)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (18)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50)\ \Omega}$
	$I_{sys} = 3{,}854\angle 77°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (19)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 77°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 77°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (20)	$V_S = E_S - \left(Z_S \times I_{sys}\right)$
	$V_S = 92{,}953\angle 120°\ V - [(2 + j10\ )\Omega \times 3{,}854\angle 77°\ A]$
	$V_S = 65{,}271\angle 99°\ V$
The impedance seen by the relay on Z_L.	
Eq. (21)	$Z_{L-Relay} = \frac{V_S}{I_L}$

Table 3: Example Calculation (Lens Point 2)	
	$Z_{L-Relay} = \frac{65{,}271\angle 99° \, V}{3{,}854\angle 77° \, A}$
	$Z_{L-Relay} = 15.676 + j6.41 \, \Omega$

Table 4: Example Calculation (Lens Point 3)			
This example is for calculating the impedance third point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (22)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120° \, V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120° \, V$		
Eq. (23)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0° \, V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0° \, V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10 \, \Omega$	$Z_L = 4 + j20 \, \Omega$	$Z_R = 4 + j20 \, \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10} \, \Omega$		
Total impedance between the generators.			
Eq. (24)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20) \, \Omega \times (4 + j20) \times 10^{10} \, \Omega\right)}{\left((4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega\right)}$		
	$Z_{total} = 4 + j20 \, \Omega$		
Total system impedance.			
Eq. (25)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10) \, \Omega + (4 + j20) \, \Omega + (4 + j20) \, \Omega$		
	$Z_{sys} = 10 + j50 \, \Omega$		

Table 4: Example Calculation (Lens Point 3)	
Total system current from sending-end source.	
Eq. (26)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 92{,}953.7\angle 0°\ V}{(10 + j50)\ \Omega}$
	$I_{sys} = 3{,}854\angle 65.5°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (27)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 65.5°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 65.5°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (28)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 120°\ V - [(2 + j10)\ \Omega \times 3{,}854\angle 65.5°\ A]$
	$V_S = 98{,}265\angle 110.6°\ V$
The impedance seen by the relay on Z_L.	
Eq. (29)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle 110.6°\ V}{3{,}854\angle 65.5°\ A}$
	$Z_{L-Relay} = 18.005 + j18.054\ \Omega$

Table 5: Example Calculation (Lens Point 4)	
This example is for calculating the impedance fourth point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 240 degrees. See Figures 3 and 4.	
Eq. (30)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 240°\ V}{\sqrt{3}}$

Table 5: Example Calculation (Lens Point 4)			
	$E_S = 132{,}791\angle 240°\ V$		
Eq. (31)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (32)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (33)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (34)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240°\ V - 132{,}791\angle 0°\ V}{(10 + j50\ )\Omega}$		
	$I_{sys} = 4{,}511\angle 131.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (35)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 131.1°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$		
	$I_L = 4{,}511\angle 131.1°\ A$		

Table 5: Example Calculation (Lens Point 4)			
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.			
Eq. (36)	$V_S = E_S - (Z_S \times I_L)$		
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10\,)\,\Omega \times 4{,}511\angle 131.1° \, A]$		
	$V_S = 95{,}756\angle -106.1° \, V$		
The impedance seen by the relay on Z_L.			
Eq. (37)	$Z_{L-Relay} = \frac{V_S}{I_L}$		
	$Z_{L-Relay} = \frac{95{,}756\angle -106.1° \, V}{4{,}511\angle 131.1° \, A}$		
	$Z_{L-Relay} = -11.434 + j17.887\ \Omega$		

Table 6: Example Calculation (Lens Point 5)			
This example is for calculating the impedance fifth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (38)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 240° \, V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 240° \, V$		
Eq. (39)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \, V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \, V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (40)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		

Table 6: Example Calculation (Lens Point 5)	
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (41)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10\ \Omega) + (4 + j20\ \Omega) + (4 + j20\ \Omega)$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (42)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 240°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$
	$I_{sys} = 3{,}854\angle 125.5°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (43)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 125.5°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 125.5°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (44)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 92{,}953.7\angle 240°\ V - [(2 + j10\ )\ \Omega \times 3{,}854\angle 125.5°\ A]$
	$V_S = 65{,}270.5\angle -99.4°\ V$
The impedance seen by the relay on Z_L.	
Eq. (45)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{65{,}270.5\angle -99.4°\ V}{3{,}854\angle 125.5°\ A}$
	$Z_{L-Relay} = -12.005 + j11.946\ \Omega$

Table 7: Example Calculation (Lens Point 6)			
This example is for calculating the impedance sixth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (46)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 240°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 240°\ V$		
Eq. (47)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (48)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (49)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (50)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240°\ V - 92{,}953.7\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 3{,}854\angle 137.1°\ A$		

Table 7: Example Calculation (Lens Point 6)	
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (51)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 137.1° \, A \times \frac{(4 + j20) \times 10^{10} \, \Omega}{(4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega}$
	$I_L = 3{,}854\angle 137.1° \, A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (52)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10 \,) \, \Omega \times 3{,}854\angle 137.1° \, A]$
	$V_S = 98{,}265\angle -110.6° \, V$
The impedance seen by the relay on Z_L.	
Eq. (53)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle -110.6° \, V}{3{,}854\angle 137.1° \, A}$
	$Z_{L-Relay} = -9.676 + j23.59 \, \Omega$

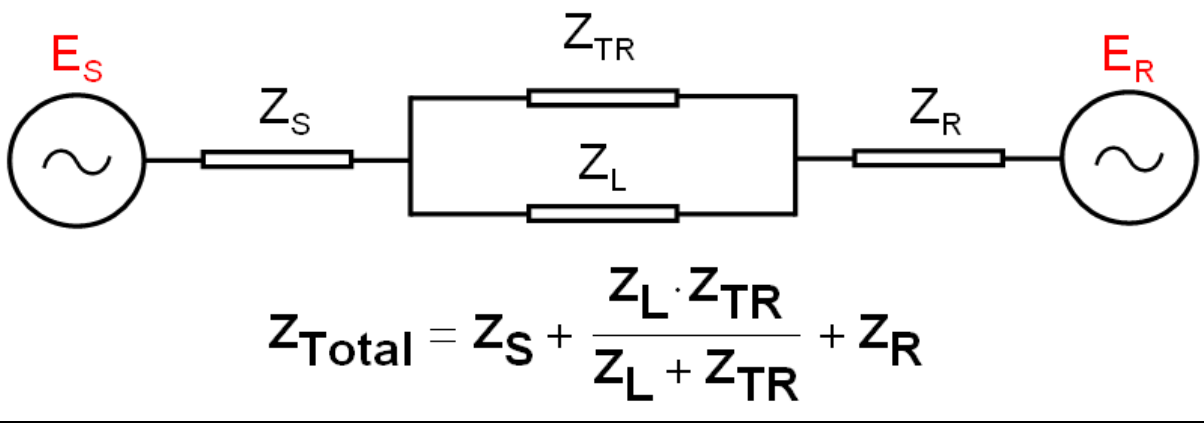


Figure 6: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, line impedance Z_L, and parallel transfer impedance Z_{TR}.

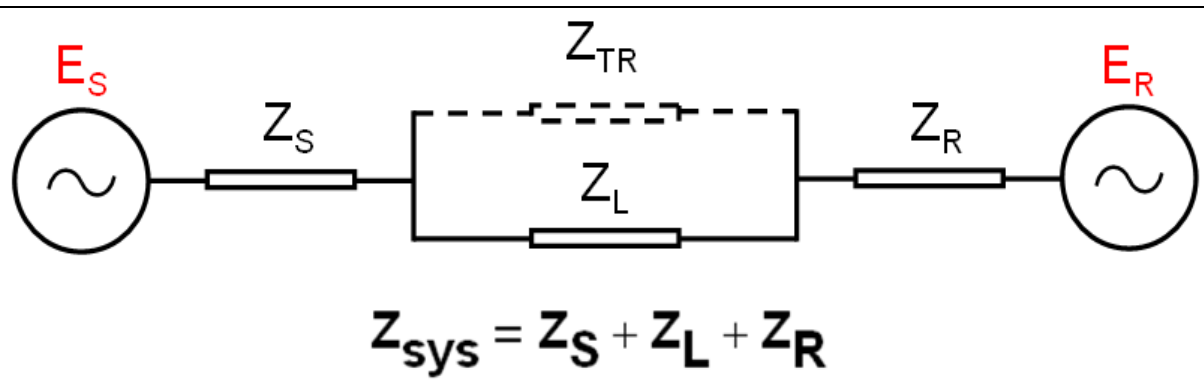


Figure 7: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, and line impedance Z_L with the parallel transfer impedance Z_{TR} removed.

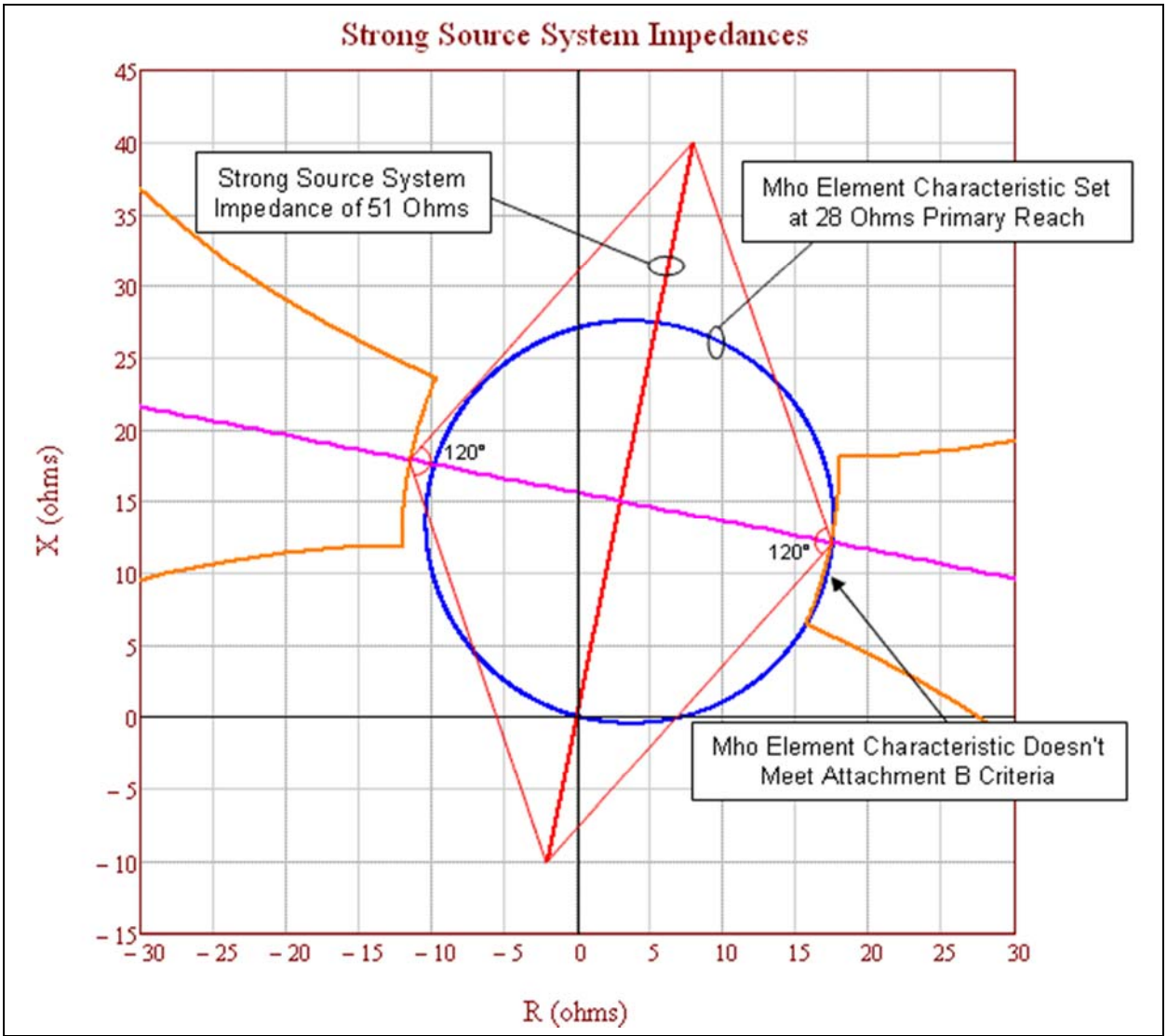


Figure 8: A strong-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) does not meet the PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 8 above represents a heavily-loaded system with all generation in service and all transmission BES Elements in their normal operating state. The mho element characteristic (set at 137% of Z_L) extends into the unstable power swing region (i.e., the orange characteristic). Using the strongest source system is more conservative because it shrinks the unstable power swing region, bringing it closer to the mho element characteristic. This figure also graphically represents the effect of a system strengthening over time and this is the reason for re-evaluation if the relay has not been evaluated in the last five calendar years. Figure 9 below depicts a relay that meets the PRC-026-1 – Attachment B, Criterion A. Figure 8 depicts the same relay with the same setting five years later, where each source has strengthened by about 10% and now the same mho element characteristic does not meet Criterion A.

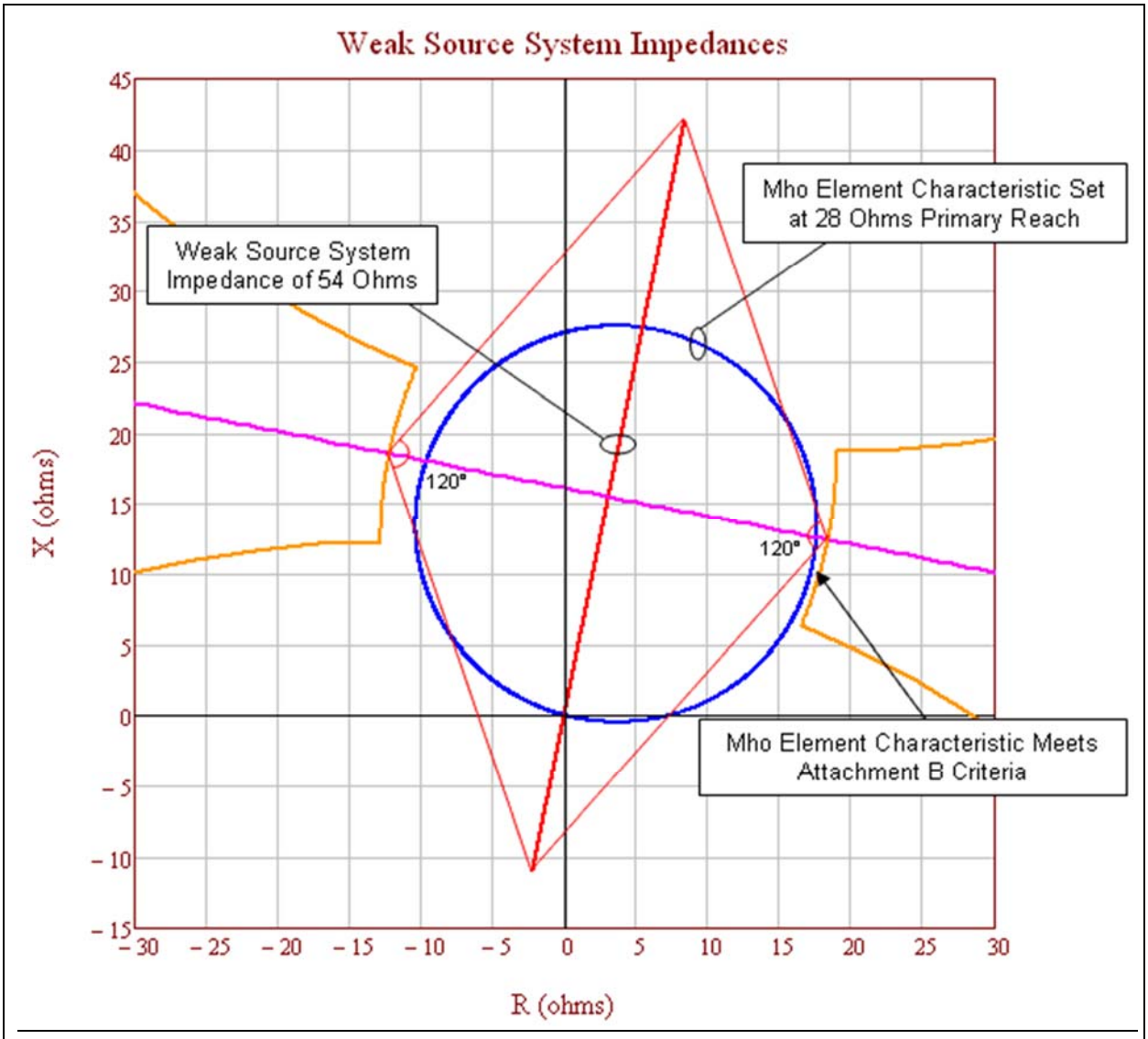


Figure 9: A weak-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) meets the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 9 above represents a lightly-loaded system, using a minimum generation profile. The mho element characteristic (set at 137% of Z_L) does not extend into the unstable power swing region (i.e., the orange characteristic). Using a weaker source system expands the unstable power swing region away from the mho element characteristic.

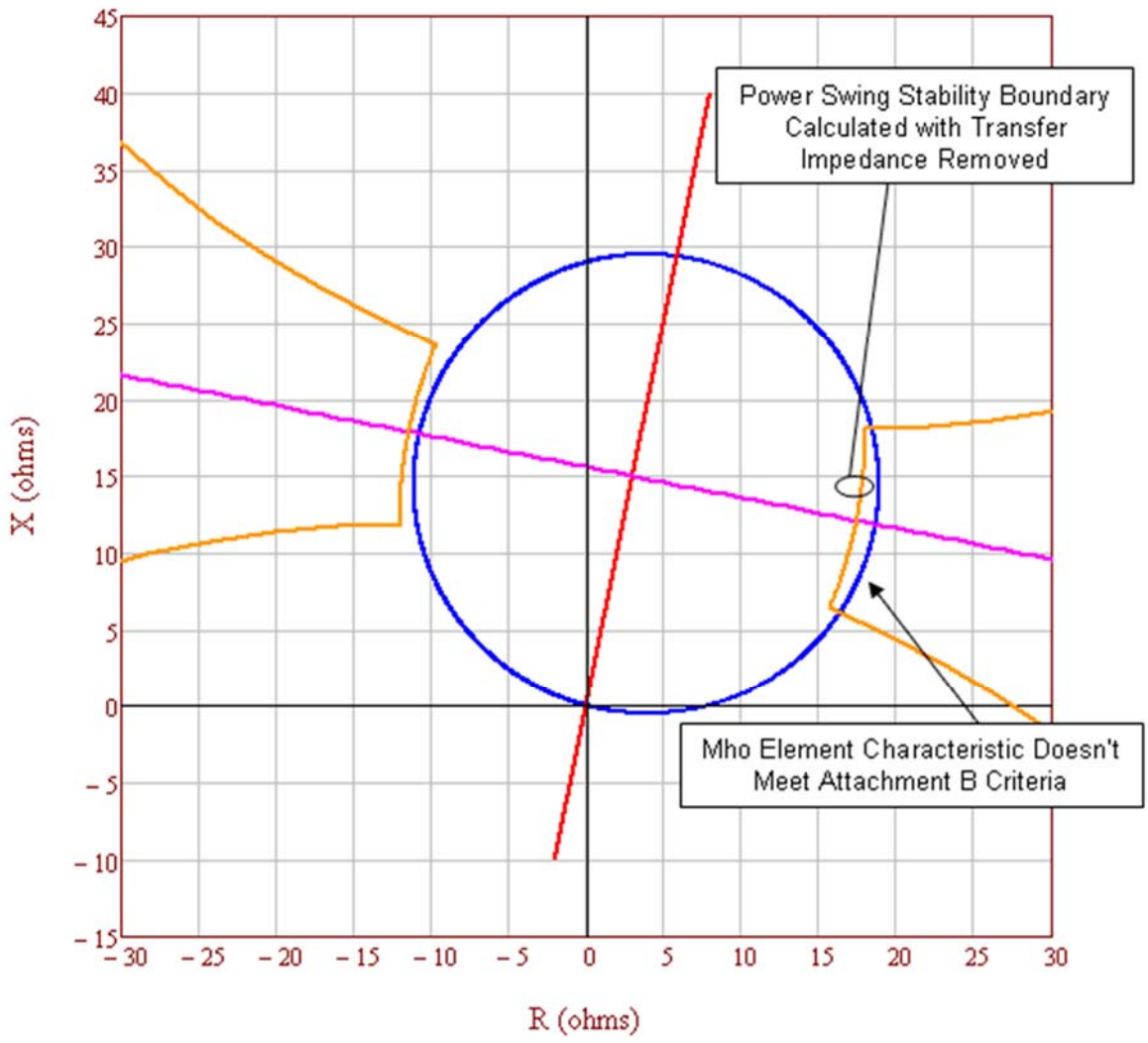


Figure 10: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance removed. This relay mho element characteristic (i.e., the blue circle) does not meet PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region.

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
Calculations for the point at 120 degrees with equal source impedances. The total system current equals the line current. See Figure 10.	
Eq. (54)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$
	$E_S = 132{,}791\angle 120°\ V$

Table 8: Example Calculation (Parallel Transfer Impedance Removed)			
Eq. (55)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (56)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (57)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (58)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (59)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 71.3°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$		
	$I_L = 4{,}511\angle 71.3°\ A$		

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (60)	$V_S = E_S - \left(Z_S \times I_{sys}\right)$
	$V_S = 132{,}791\angle 120° \, V - [(2 + j10\ \Omega) \times 4{,}511\angle 71.3° \, A]$
	$V_S = 95{,}757\angle 106.1° \, V$
The impedance seen by the relay on Z_L.	
Eq. (61)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \, V}{4{,}511\angle 71.3° \, A}$
	$Z_{L-Relay} = 17.434 + j12.113\ \Omega$

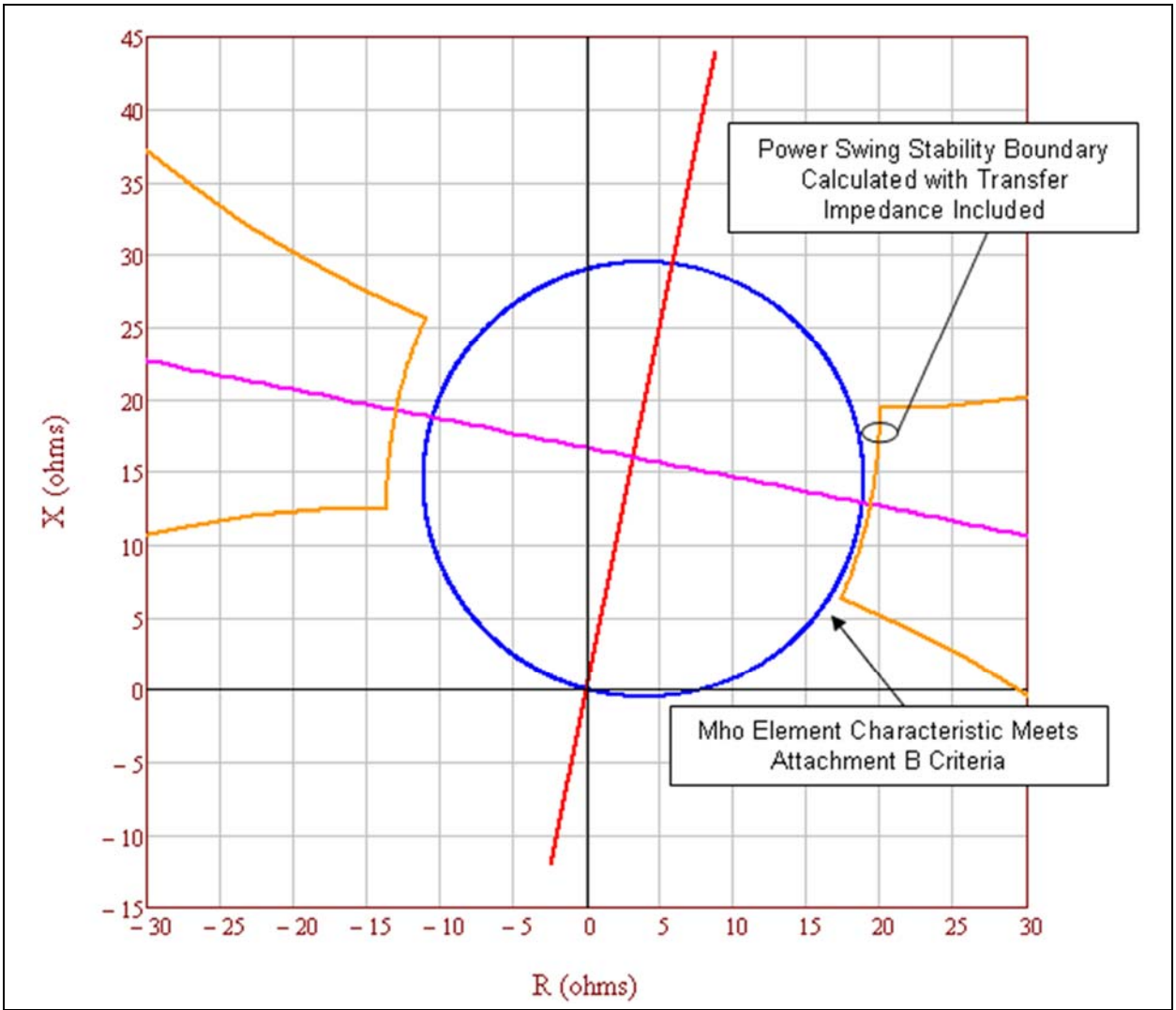


Figure 11: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance included causing the mho element characteristic (i.e., the blue circle) to appear to meet the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

In Figure 11 above, the parallel transfer impedance is 5 times the line impedance. The unstable power swing region has expanded out beyond the mho element characteristic due to the infeed effect from the parallel current through the parallel transfer impedance, thus allowing the mho element characteristic to appear to meet the PRC-026-1 – Attachment B, Criterion A. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

Table 9: Example Calculation (Parallel Transfer Impedance Included)			
Calculations for the point at 120 degrees with equal source impedances. The total system current does not equal the line current. See Figure 11.			
Eq. (62)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (63)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 5$		
	$Z_{TR} = (4 + j20)\ \Omega \times 5$		
	$Z_{TR} = 20 + j100\ \Omega$		
Total impedance between the generators.			
Eq. (64)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{(4 + j20)\ \Omega \times (20 + j100)\ \Omega}{(4 + j20)\ \Omega + (20 + j100)\ \Omega}$		
	$Z_{total} = 3.333 + j16.667\ \Omega$		
Total system impedance.			
Eq. (65)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (3.333 + j16.667)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 9.333 + j46.667\ \Omega$		
Total system current from sending-end source.			
Eq. (66)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{9.333 + j46.667\ \Omega}$		

Table 9: Example Calculation (Parallel Transfer Impedance Included)	
	$I_{sys} = 4{,}833\angle 71.3° \; A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (67)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 4{,}833\angle 71.3° \; A \times \frac{(20 + j100)\;\Omega}{(4 + j20)\;\Omega + (20 + j100)\;\Omega}$
	$I_L = 4{,}027.4\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (68)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10\;\Omega) \times 4{,}833\angle 71.3° \; A]$
	$V_S = 93{,}417\angle 104.7° \; V$
The impedance seen by the relay on Z_L.	
Eq. (69)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{93{,}417\angle 104.7° \; V}{4{,}027\angle 71.3° \; A}$
	$Z_{L-Relay} = 19.366 + j12.767\;\Omega$

Table 10: Percent Increase of a Lens Due To Parallel Transfer Impedance.	
The following demonstrates the percent size increase of the lens characteristic for Z_{TR} in multiples of Z_L with the parallel transfer impedance included.	
Z_{TR} in multiples of Z_L	Percent increase of lens with equal EMF sources (Infinite source as reference)
Infinite	N/A
1000	0.05%
100	0.46%
10	4.63%
5	9.27%
2	23.26%
1	46.76%
0.5	94.14%
0.25	189.56%

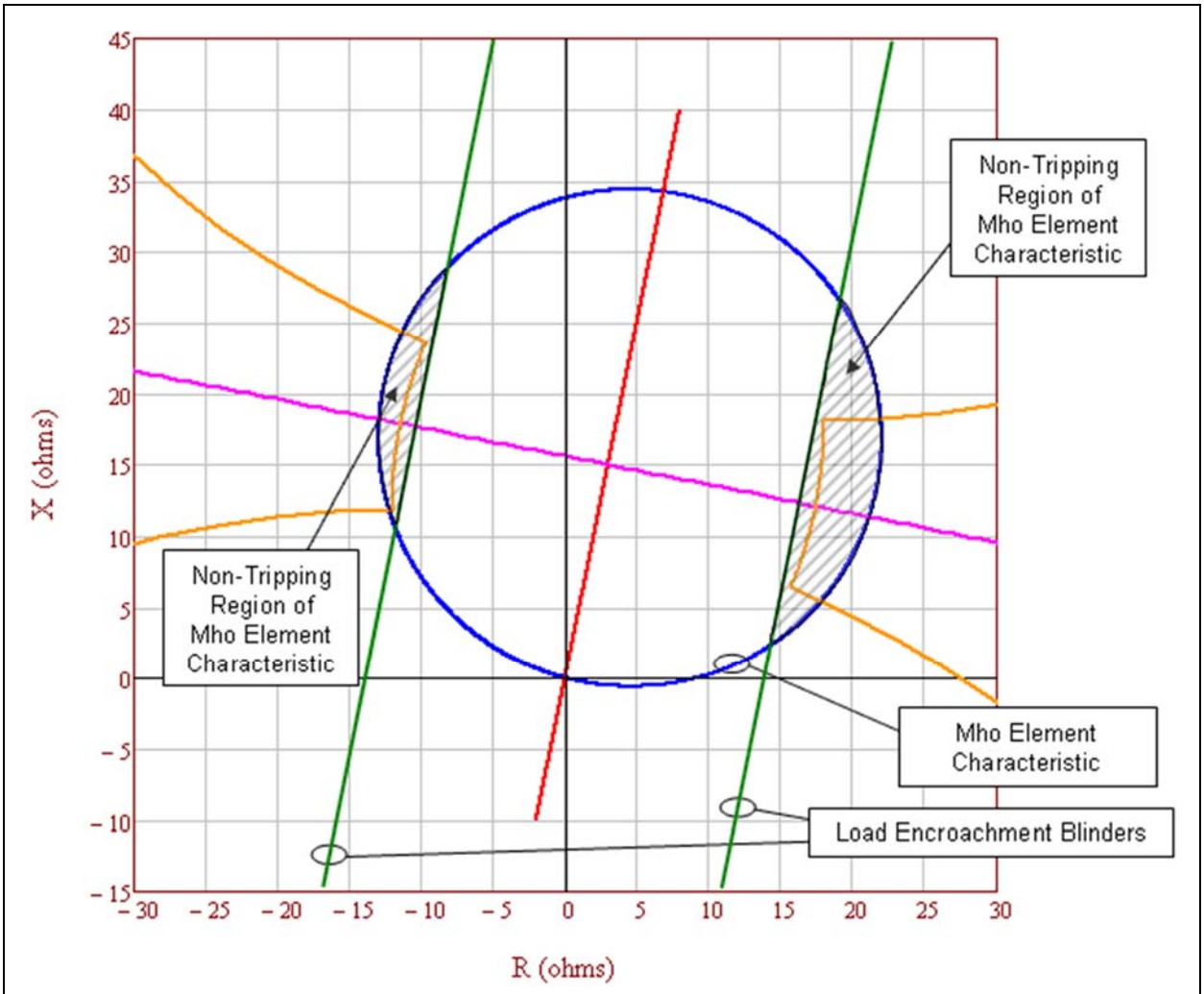


Figure 12: The tripping portion of the mho element characteristic (i.e., the blue circle) not blocked by load encroachment (i.e., the parallel green lines) is completely contained within the unstable power swing region (i.e., the orange characteristic). Therefore, the mho element characteristic meets the PRC-026-1 – Attachment B, Criterion A.

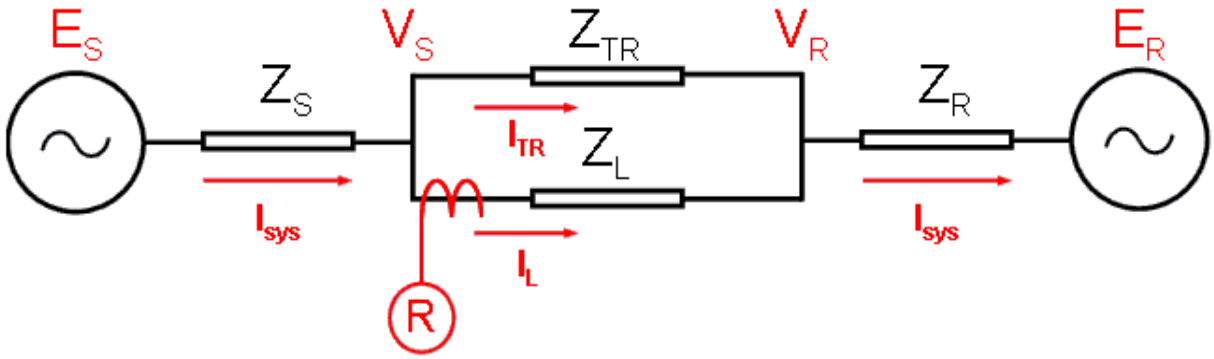


Figure 13: The infeed diagram shows the impedance in front of the relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.

Table 11: Calculations (System Apparent Impedance in the forward direction)

The following equations are provided for calculating the apparent impedance back to the E_R source voltage as seen by relay R. Infeed equations from V_S to source E_R where $E_R = 0$. See Figure 13.

Eq. (70)	$I_L = \frac{V_S - V_R}{Z_L}$			
Eq. (71)	$I_{sys} = \frac{V_R - E_R}{Z_R}$			
Eq. (72)	$I_{sys} = I_L + I_{TR}$			
Eq. (73)	$I_{sys} = \frac{V_R}{Z_R}$	Since $E_R = 0$	Rearranged:	$V_R = I_{sys} \times Z_R$
Eq. (74)	$I_L = \frac{V_S - I_{sys} \times Z_R}{Z_L}$			
Eq. (75)	$I_L = \frac{V_S - [(I_L + I_{TR}) \times Z_R]}{Z_L}$			
Eq. (76)	$V_S = (I_L \times Z_L) + (I_L \times Z_R) + (I_{TR} \times Z_R)$			
Eq. (77)	$Z_{Relay} = \frac{V_S}{I_L} = Z_L + Z_R + \frac{I_{TR} \times Z_R}{I_L} = Z_L + Z_R \times \left(1 + \frac{I_{TR}}{I_L}\right)$			
Eq. (78)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$			
Eq. (79)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$			

Table 11: Calculations (System Apparent Impedance in the forward direction)	
Eq. (80)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$
The infeed equations shows the impedance in front of the relay R (Figure 13) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.	
Eq. (81)	$Z_{Relay} = Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$

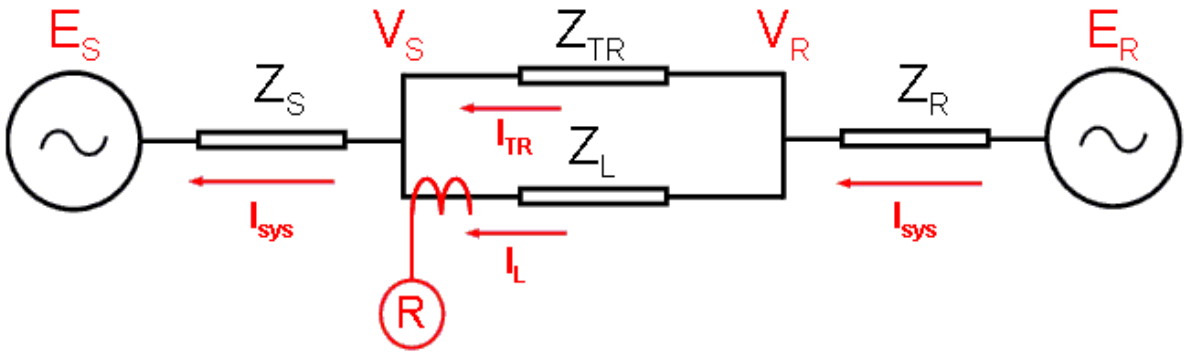


Figure 14: The infeed diagram shows the impedance behind relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)				
The following equations are provided for calculating the apparent impedance back to the E_S source voltage as seen by relay R. Infeed equations from V_R back to source E_S where $E_S = 0$. See Figure 14.				
Eq. (82)	$I_L = \frac{V_R - V_S}{Z_L}$			
Eq. (83)	$I_{sys} = \frac{V_S - E_S}{Z_S}$			
Eq. (84)	$I_{sys} = I_L + I_{TR}$			
Eq. (85)	$I_{sys} = \frac{V_S}{Z_S}$	Since $E_s = 0$	Rearranged:	$V_S = I_{sys} \times Z_S$
Eq. (86)	$I_L = \frac{V_R - I_{sys} \times Z_S}{Z_L}$			

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)		
Eq. (87)	$I_L = \frac{V_R - [(I_L + I_{TR}) \times Z_S]}{Z_L}$	
Eq. (88)	$V_R = (I_L \times Z_L) + (I_L \times Z_S) + (I_{TR} \times Z_{RS})$	
Eq. (89)	$Z_{Relay} = \frac{V_R}{I_L} = Z_L + Z_S + \frac{I_{TR} \times Z_S}{I_L} = Z_L + Z_S \times \left(1 + \frac{I_{TR}}{I_L}\right)$	
Eq. (90)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$	
Eq. (91)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$	
Eq. (92)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$	
The infeed equations shows the impedance behind relay R (Figure 14) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.		
Eq. (93)	$Z_{Relay} = Z_L + Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	As seen by relay R at the receiving-end of the line.
Eq. (94)	$Z_{Relay} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	Subtract Z_L for relay R impedance as seen at sending-end of the line.

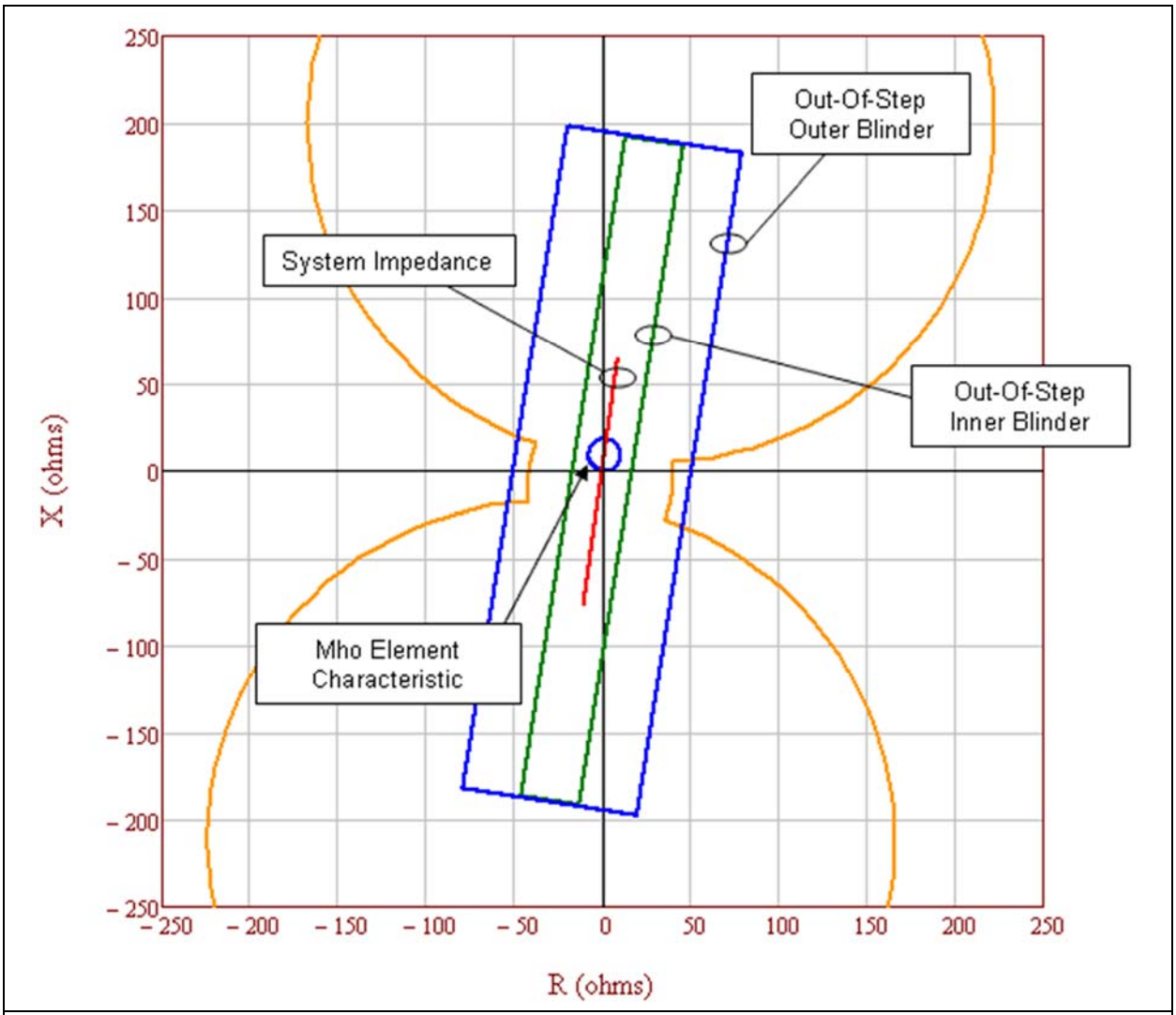


Figure 15: Out-of-step trip (OST) inner blinder (i.e., the parallel green lines) meets the PRC-026-1 – Attachment B, Criterion A because the inner OST blinder initiates tripping either On-The-Way-In or On-The-Way-Out. Since the inner blinder is completely contained within the unstable power swing region (i.e., the orange characteristic), it meets the PRC-026-1 – Attachment B, Criterion A.

Table 13: Example Calculation (Voltage Ratios)			
These calculations are based on the loss-of-synchronism characteristics for the cases of N < 1 and N > 1 as found in the *Application of Out-of-Step Blocking and Tripping Relays*, GER-3180, p. 12, Figure 3.[18] The GE illustration shows the formulae used to calculate the radius and center of the circles that make up the ends of the portion of the lens.			
Voltage ratio equations, source impedance equation with infeed formulae applied, and circle equations.			
Given:	$E_S = 0.7$	$E_R = 1.0$	
Eq. (95)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{0.7}{1.0} = 0.7$		
The total system impedance as seen by the relay with infeed formulae applied.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
	$Z_{TR} = (4 + j20) \times 10^{10}\ \Omega$		
Eq. (96)	$Z_{sys} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right) + \left[Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right]$		
	$Z_{sys} = 10 + j50\ \Omega$		
The calculated coordinates of the lower loss-of-synchronism circle center.			
Eq. (97)	$Z_{C1} = -\left[Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right] - \left[\frac{N^2 \times Z_{sys}}{1 - N^2}\right]$		
	$Z_{C1} = -\left[(2 + j10)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega}\right)\right] - \left[\frac{0.7^2 \times (10 + j50)\ \Omega}{1 - 0.7^2}\right]$		
	$Z_{C1} = -11.608 - j58.039\ \Omega$		
The calculated radius of the lower loss-of-synchronism circle.			
Eq. (98)	$r_a = \left\lvert \frac{N \times Z_{sys}}{1 - N^2} \right\rvert$		
	$r_a = \left\lvert \frac{0.7 \times (10 + j50)\ \Omega}{1 - 0.7^2} \right\rvert$		
	$r_a = 69.987\ \Omega$		
The calculated coordinates of the upper loss-of-synchronism circle center.			
Given:	$E_S = 1.0$	$E_R = 0.7$	

[18] http://store.gedigitalenergy.com/faq/Documents/Alps/GER-3180.pdf

Table 13: Example Calculation (Voltage Ratios)	
Eq. (99)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{1.0}{0.7} = 1.43$
Eq. (100)	$Z_{C2} = Z_L + \left[Z_R \times \left(1 + \frac{Z_L}{Z_{TR}} \right) \right] + \left[\frac{Z_{sys}}{N^2 - 1} \right]$
	$Z_{C2} = 4 + j20\ \Omega + \left[(4 + j20)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega} \right) \right] + \left[\frac{(10 + j50)\ \Omega}{1.43^2 - 1} \right]$
	$Z_{C2} = 17.608 + j88.039\ \Omega$
The calculated radius of the upper loss-of-synchronism circle.	
Eq. (101)	$r_b = \left\lvert \frac{N \times Z_{sys}}{N^2 - 1} \right\rvert$
	$r_b = \left\lvert \frac{1.43 \times (10 + j50)\ \Omega}{1.43^2 - 1} \right\rvert$
	$r_b = 69.987\ \Omega$

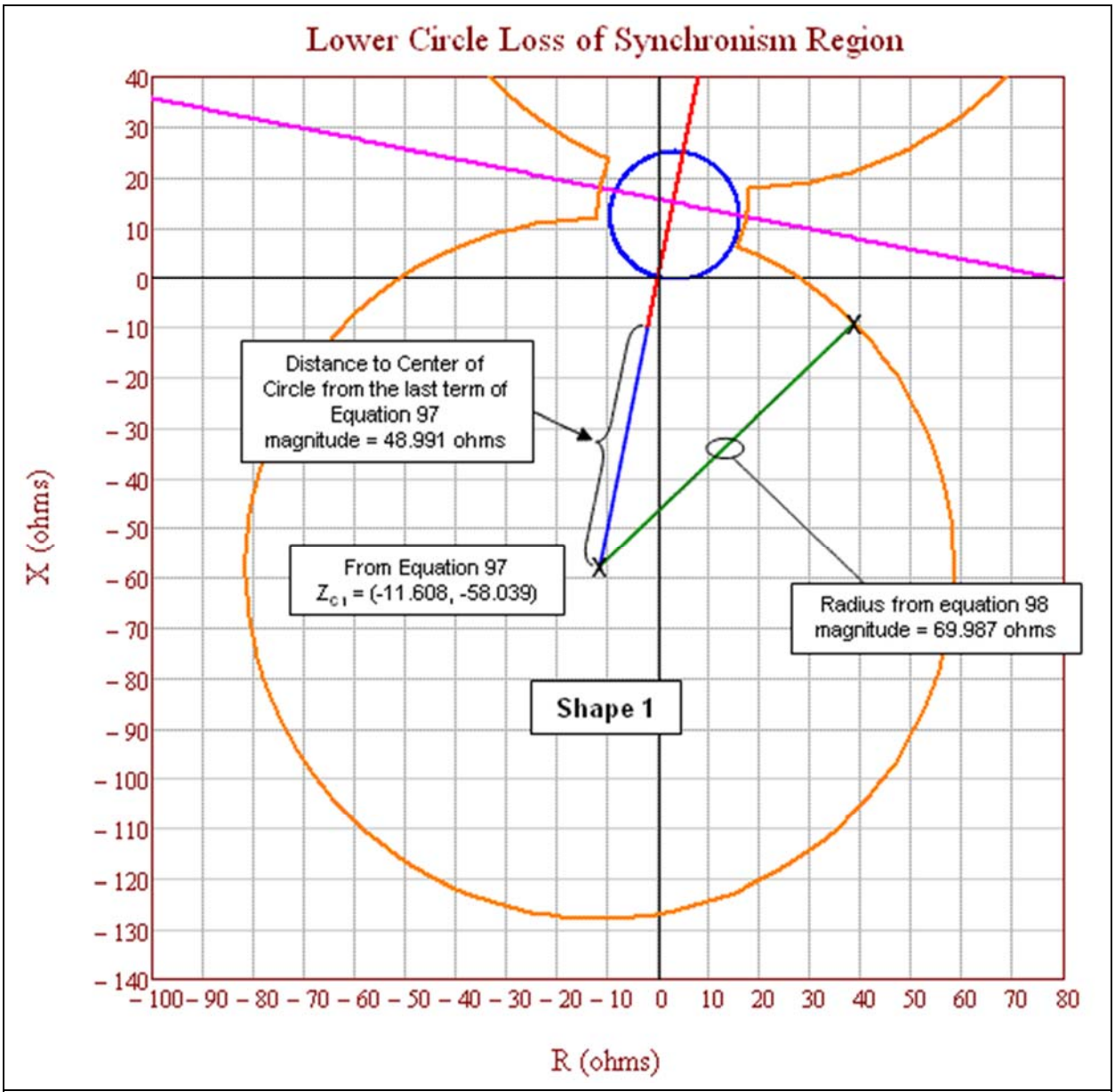


Figure 15a: Lower circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

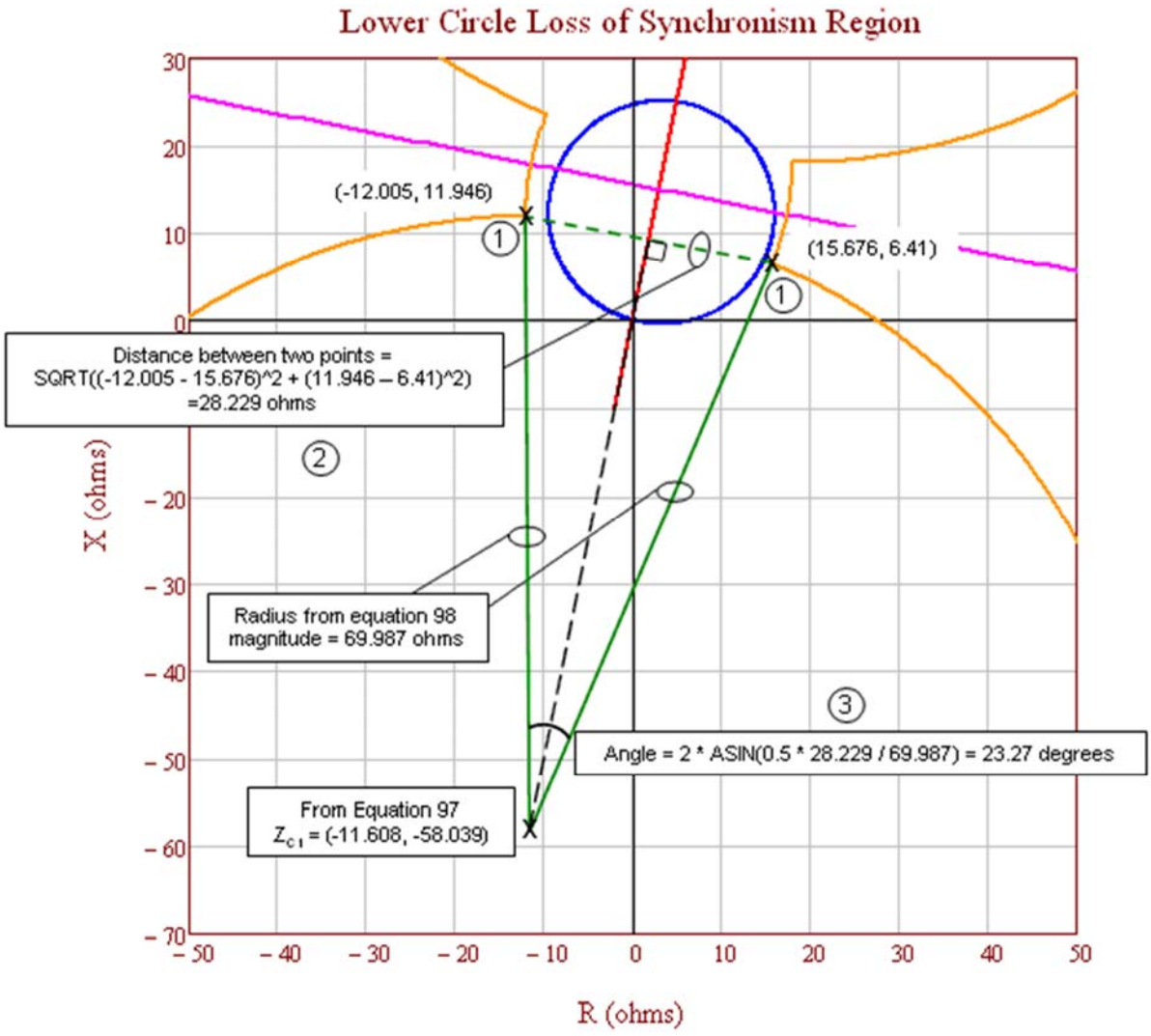


Figure 15b: Lower circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the lower circle loss-of-synchronism points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 0.7 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two lower circle loss-of-synchronism points identified in Step 1. 3) Calculate the angle of arc that connects the two lower circle loss-of-synchronism points identified in Step 1.

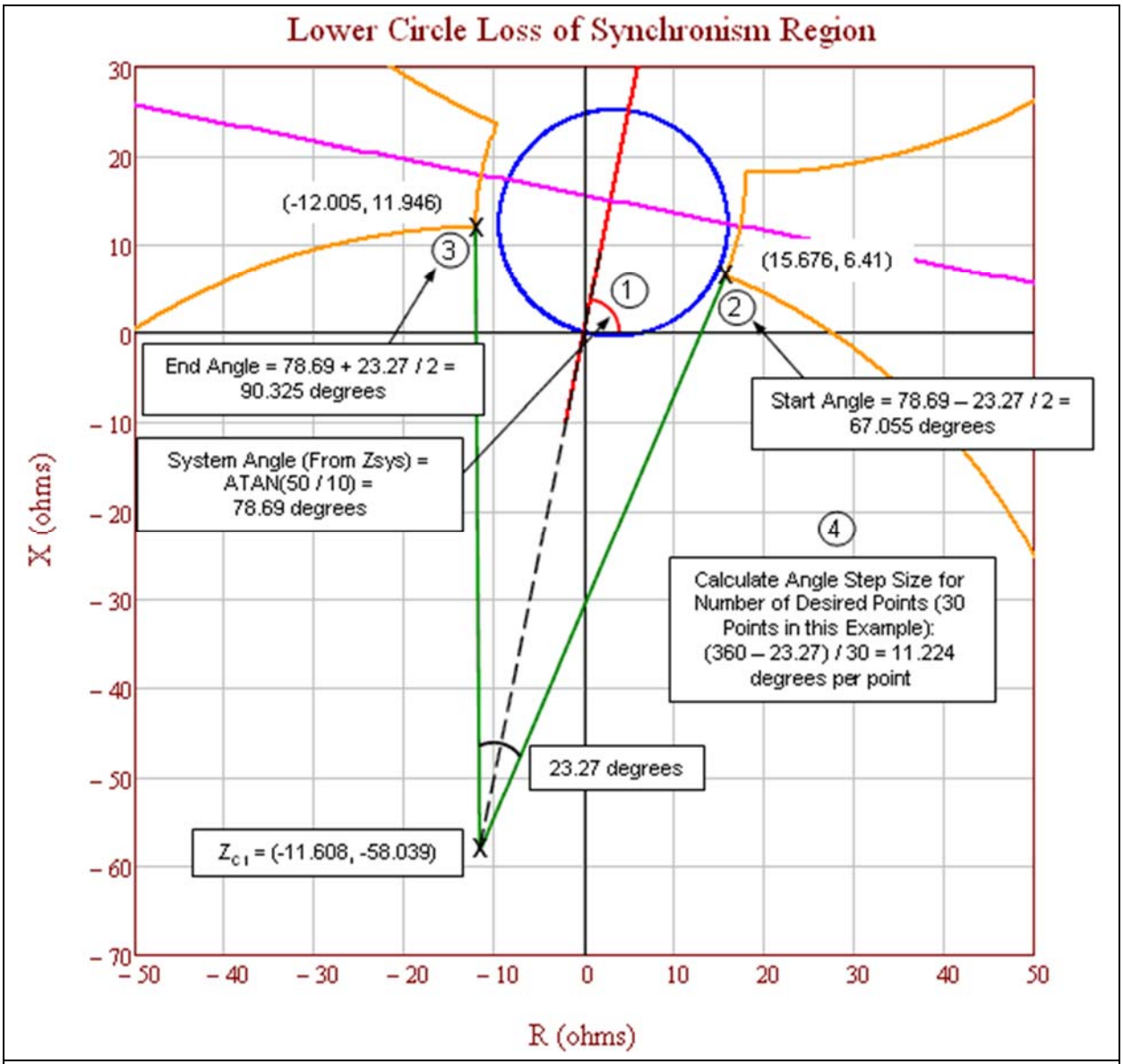


Figure 15c: Lower circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

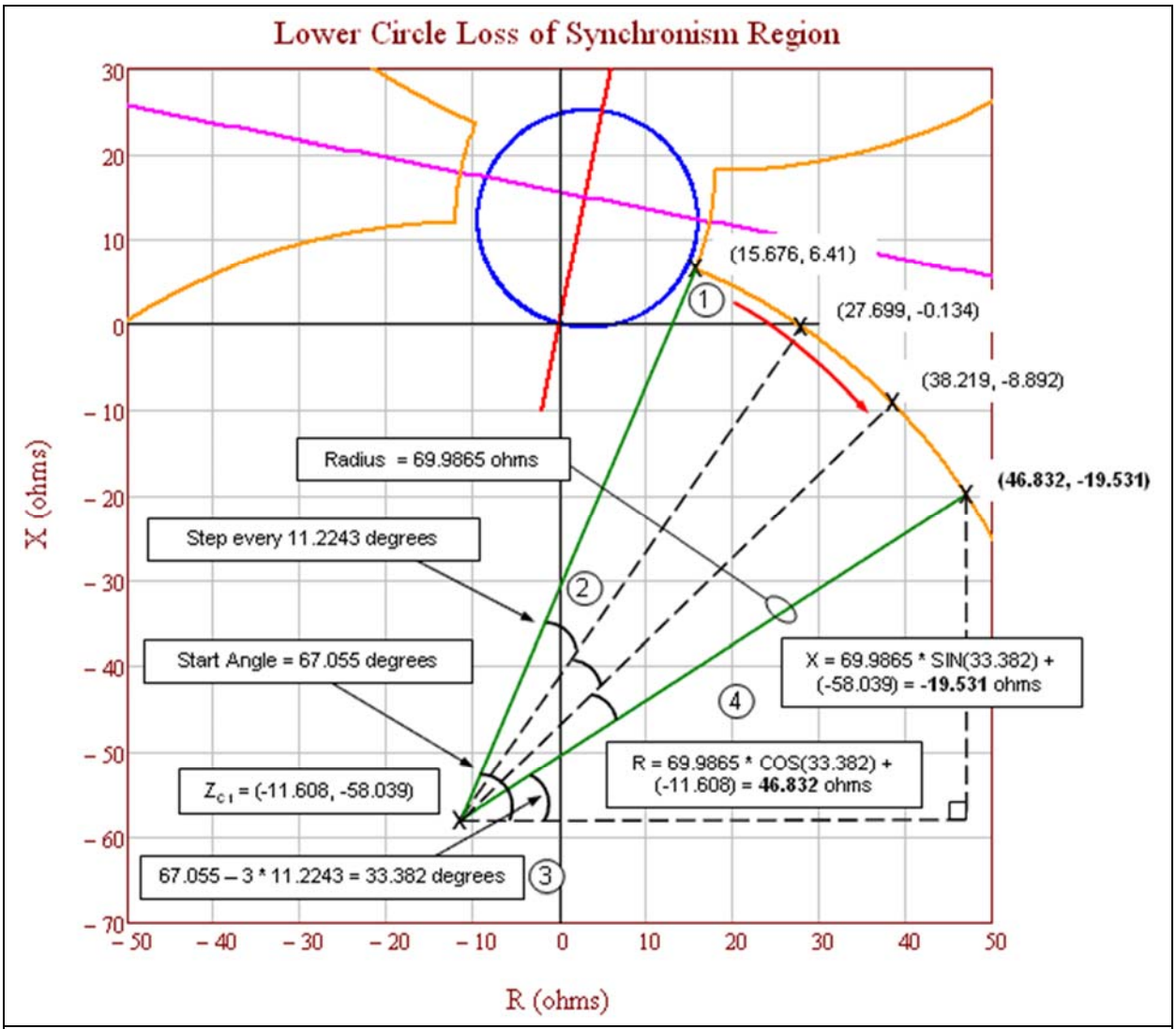


Figure 15d: Lower circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R–X coordinates.

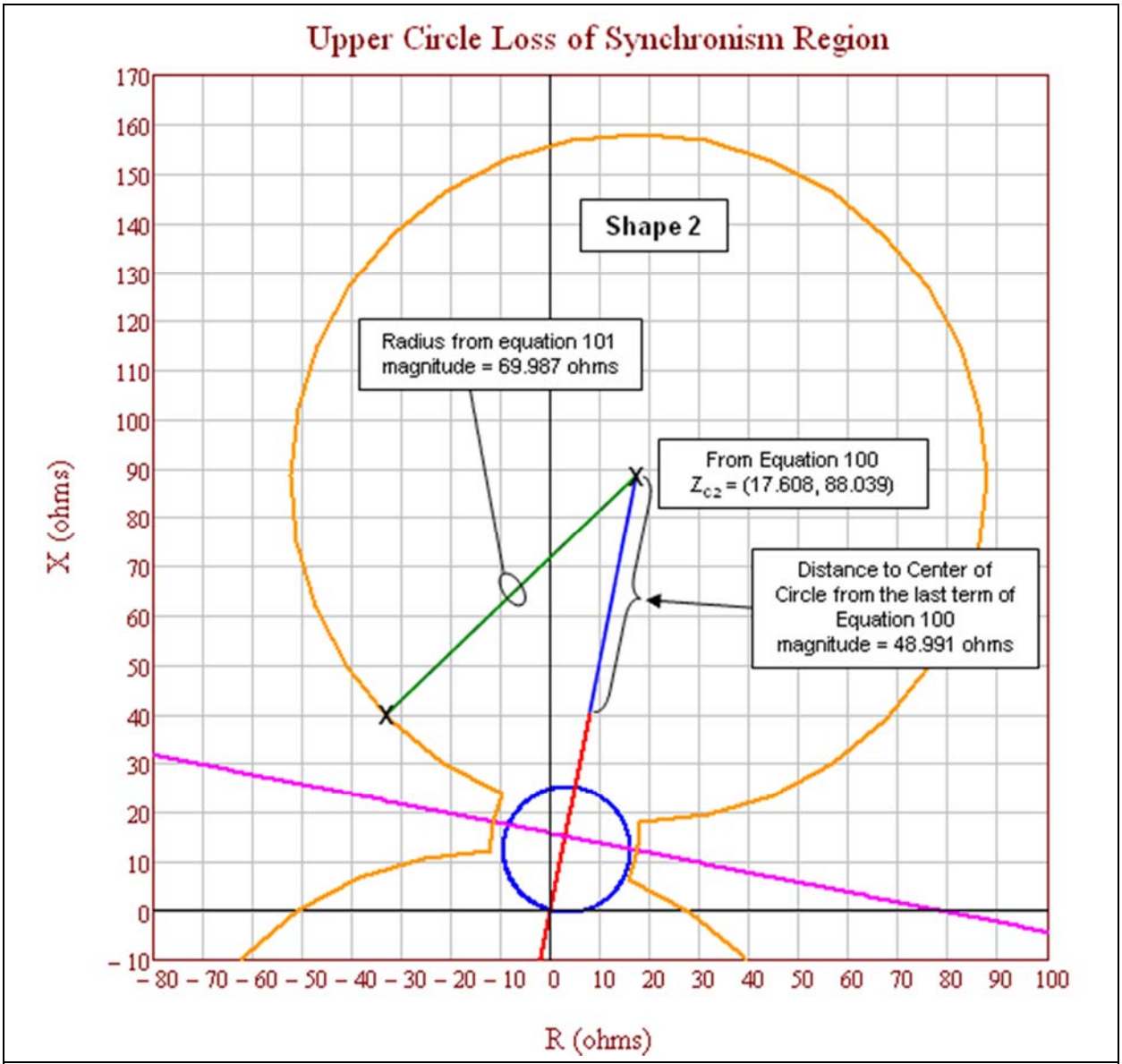


Figure 15e: Upper circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

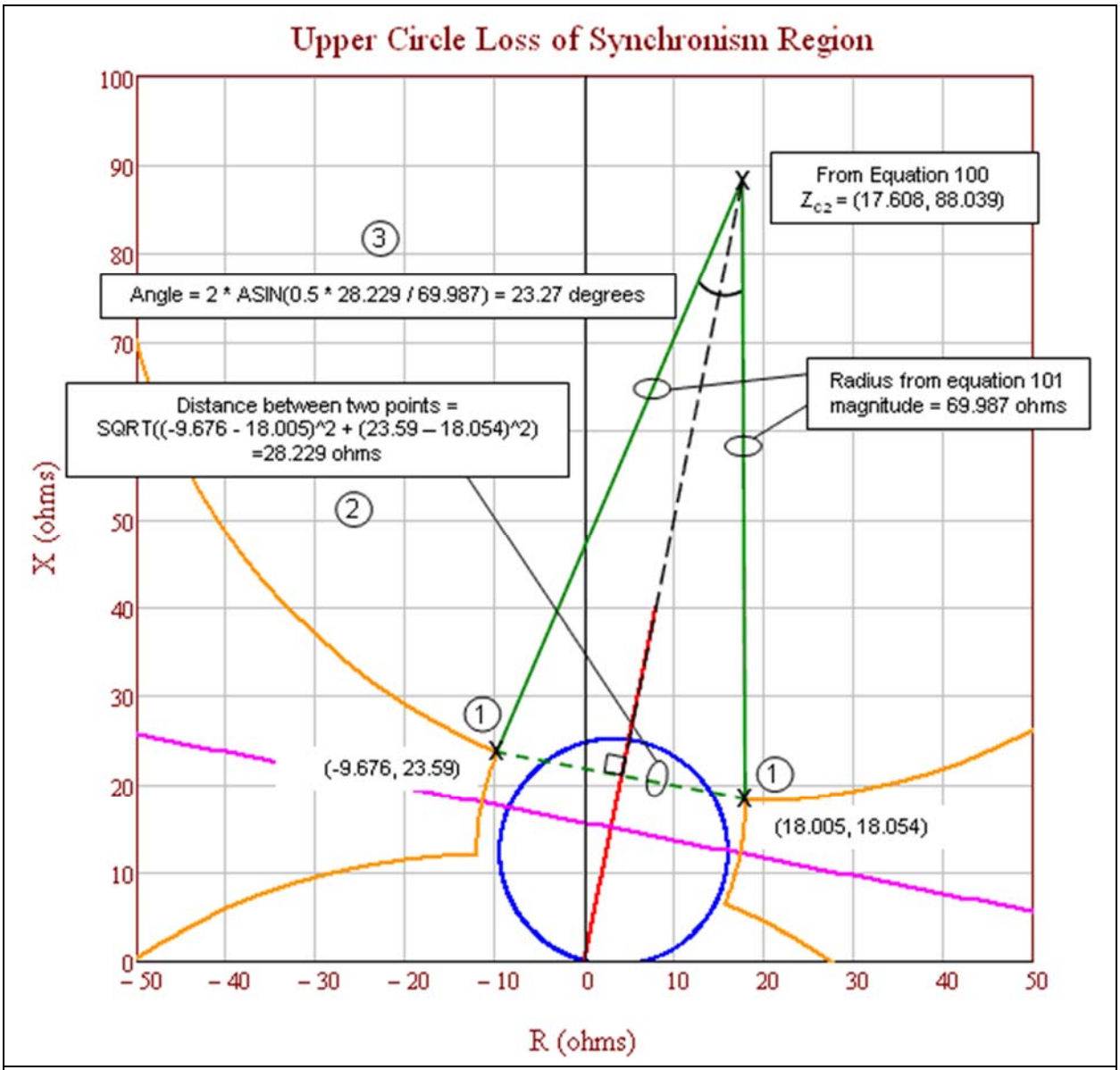


Figure 15f: Upper circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the upper circle points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 1.43 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two upper circle points identified in Step 1. 3) Calculate the angle of arc that connects the two upper circle points identified in Step 1.

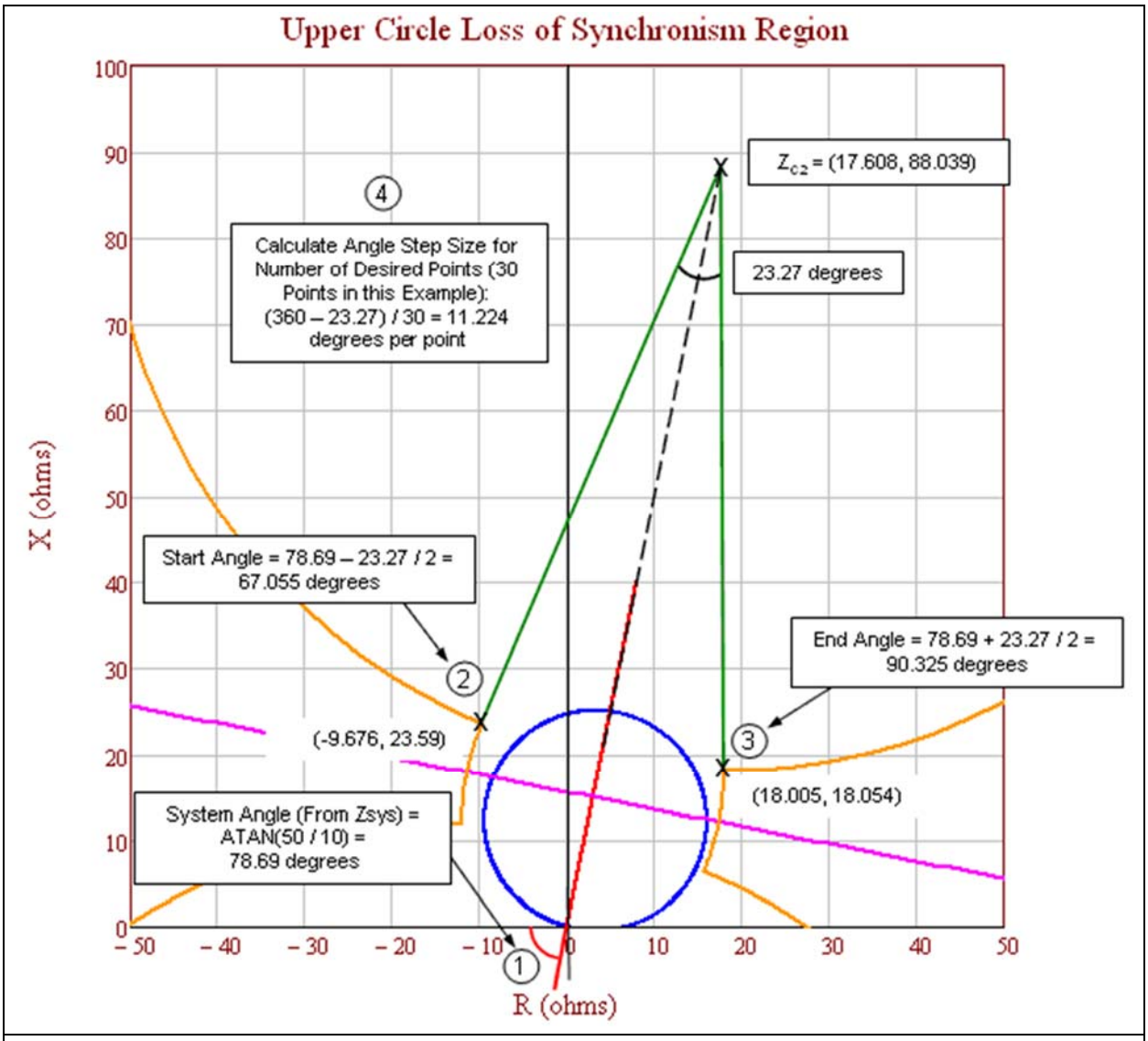


Figure 15g: Upper circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

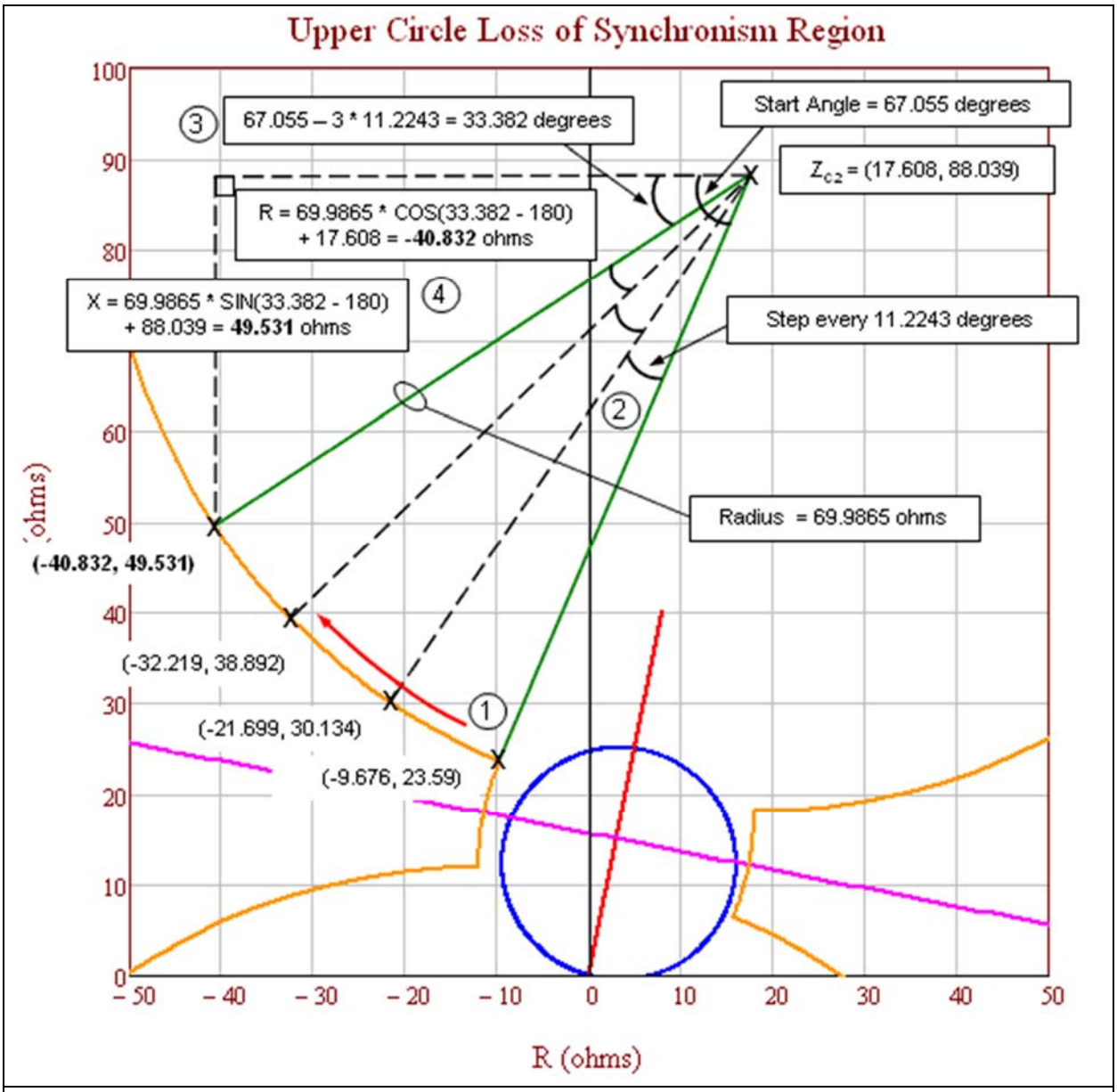


Figure 15h: Upper circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R-X coordinates.

Lower Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	15.676	6.41
55.831	27.699	-0.134
44.606	38.219	-8.892
33.382	**46.832**	**-19.531**
22.158	53.21	-31.643
10.933	57.108	-44.765
359.709	58.378	-58.395
348.485	56.97	-72.011
337.26	52.939	-85.092
326.036	46.438	-97.139
314.812	37.717	-107.69
303.587	27.109	-116.341
292.363	15.02	-122.762
281.139	1.913	-126.707
269.914	-11.712	-128.026
258.69	-25.333	-126.667
247.466	-38.429	-122.682
236.241	-50.499	-116.225
225.017	-61.081	-107.542
213.793	-69.771	-96.965
202.568	-76.235	-84.899
191.344	-80.227	-71.806
180.12	-81.594	-58.185
168.895	-80.284	-44.56
157.671	-76.347	-31.45
146.447	-69.933	-19.357
135.222	-61.288	-8.744
123.998	-50.742	-0.016
112.774	-38.699	6.491
101.549	-25.62	10.53
90.325	-12.005	11.946

Upper Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	-9.676	23.59
55.831	-21.699	30.134
44.606	-32.219	38.892
33.382	**-40.832**	**49.531**
22.158	-47.21	61.643
10.933	-51.108	74.765
359.709	-52.378	88.395
348.485	-50.97	102.011
337.26	-46.939	115.092
326.036	-40.438	127.139
314.812	-31.717	137.69
303.587	-21.109	146.341
292.363	-9.02	152.762
281.139	4.087	156.707
269.914	17.712	158.026
258.69	31.333	156.667
247.466	44.429	152.682
236.241	56.499	146.225
225.017	67.081	137.542
213.793	75.771	126.965
202.568	82.235	114.899
191.344	86.227	101.806
180.12	87.594	88.185
168.895	86.284	74.56
157.671	82.347	61.45
146.447	75.933	49.357
135.222	67.288	38.744
123.998	56.742	30.016
112.774	44.699	23.509
101.549	31.62	19.47
90.325	18.005	18.054

Figure 15i: Full tables of calculated lower and upper loss-of-synchronism circle coordinates. The highlighted row is the detailed calculated points in Figures 15d and 15h.

Application Specific to Criterion B

The PRC-026-1 – Attachment B, Criterion B evaluates overcurrent elements used for tripping. The same criteria as PRC-026-1 – Attachment B, Criterion A is used except for an additional criterion (No. 4) that calculates a current magnitude based upon generator internal voltage of 1.05 per unit. A value of 1.05 per unit generator voltage is used to establish a minimum pickup current value for overcurrent relays that have a time delay less than 15 cycles. The sending-end and receiving-end voltages are established at 1.05 per unit at 120 degree system separation angle. The 1.05 per unit is the typical upper end of the operating voltage, which is also consistent with the maximum power

transfer calculation using actual system source impedances in the PRC-023 NERC Reliability Standard. The formulas used to calculate the current are in Table 14 below.

Table 14: Example Calculation (Overcurrent)

This example is for a 230 kV line terminal with a directional instantaneous phase overcurrent element set to 50 amps secondary times a CT ratio of 160:1 that equals 8,000 amps, primary. The following calculation is where V_S equals the base line-to-ground sending-end generator source voltage times 1.05 at an angle of 120 degrees, V_R equals the base line-to-ground receiving-end generator internal voltage times 1.05 at an angle of 0 degrees, and Z_{sys} equals the sum of the sending-end source, line, and receiving-end source impedances in ohms.

Here, the instantaneous phase setting of 8,000 amps is greater than the calculated system current of 5,716 amps; therefore, it meets PRC-026-1 – Attachment B, Criterion B.

Eq. (102)	$V_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 1.05$		
	$V_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}} \times 1.05$		
	$V_S = 139{,}430\angle 120°\ V$		
Receiving-end generator terminal voltage.			
Eq. (103)	$V_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 1.05$		
	$V_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 1.05$		
	$V_R = 139{,}430\angle 0°\ V$		
The total impedance of the system (Z_{sys}) equals the sum of the sending-end source impedance (Z_S), the impedance of the line (Z_L), and receiving-end impedance (Z_R) in ohms.			
Given:	$Z_S = 3 + j26\ \Omega$	$Z_L = 1.3 + j8.7\ \Omega$	$Z_R = 0.3 + j7.3\ \Omega$
Eq. (104)	$Z_{sys} = Z_S + Z_L + Z_R$		
	$Z_{sys} = (3 + j26)\ \Omega + (1.3 + j8.7)\ \Omega + (0.3 + j7.3)\ \Omega$		
	$Z_{sys} = 4.6 + j42\ \Omega$		
Total system current.			
Eq. (105)	$I_{sys} = \frac{(V_S - V_R)}{Z_{sys}}$		
	$I_{sys} = \frac{(139{,}430\angle 120°\ V - 139{,}430\angle 0°\ V)}{(4.6 + j42)\ \Omega}$		
	$I_{sys} = 5{,}715.82\angle 66.25°\ A$		

Application Specific to Three-Terminal Lines

If a three-terminal line is identified as an Element that is susceptible to a power swing based on Requirement R1, the load-responsive protective relays at each end of the three-terminal line must be evaluated.

As shown in Figure 15j, the source impedances at each end of the line can be obtained from the similar short circuit calculation as for the two-terminal line (assuming the parallel transfer impedances are ignored).

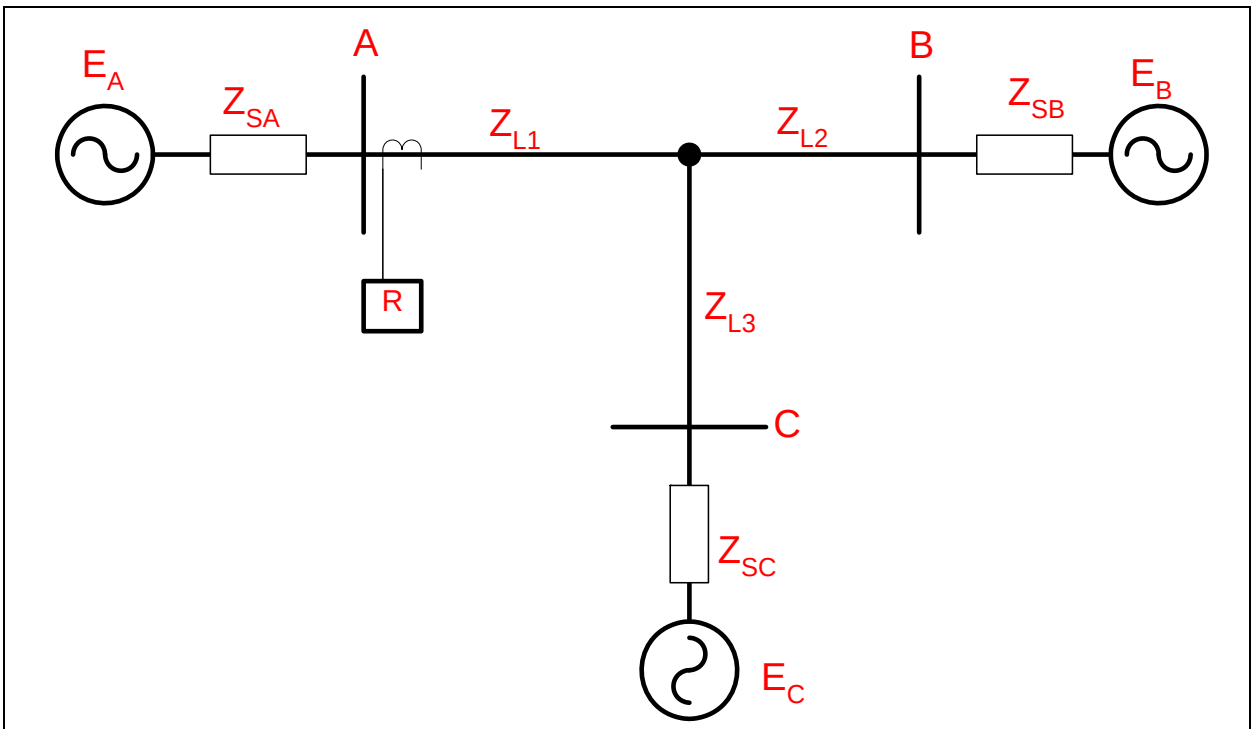


Figure 15j: Three-terminal line. To evaluate the load-responsive protective relays on the three-terminal line at Terminal A, the circuit in Figure 15j is first reduced to the equivalent circuit shown in Figure 15k. The evaluation process for the load-responsive protective relays on the line at Terminal A will now be the same as that of the two-terminal line.

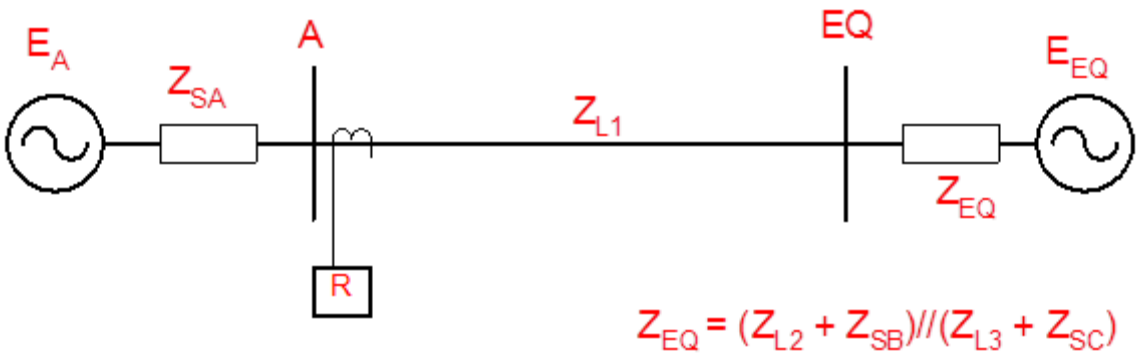


Figure 15k: Three-terminal line reduced to a two-terminal line.

Application to Generation Elements

As with transmission BES Elements, the determination of the apparent impedance seen at an Element located at, or near, a generation Facility is complex for power swings due to various interdependent quantities. These variances in quantities are caused by changes in machine internal voltage, speed governor action, voltage regulator action, the reaction of other local generators, and the reaction of other interconnected transmission BES Elements as the event progresses through the time domain. Though transient stability simulations may be used to determine the apparent impedance for verifying load-responsive relay settings,[19,20] Requirement R2, PRC-026-1 – Attachment B, Criteria A and B provides a simplified method for evaluating the load-responsive protective relay's susceptibility to tripping in response to a stable power swing without requiring stability simulations.

In general, the electrical center will be in the transmission system for cases where the generator is connected through a weak transmission system (high external impedance). In other cases where the generator is connected through a strong transmission system, the electrical center could be inside the unit connected zone.[21] In either case, load-responsive protective relays connected at the generator terminals or at the high-voltage side of the generator step-up (GSU) transformer may be challenged by power swings. Relays that may be challenged by power swings will be determined by the Planning Coordinator in Requirement R1 or by the Generator Owner after becoming aware of a generator, transformer, or transmission line BES Element that tripped[22] in response to a stable or unstable power swing due to the operation of its protective relay(s) in Requirement R2.

[19] Donald Reimert, *Protective Relaying for Power Generation Systems*, Boca Raton, FL, CRC Press, 2006.

[20] Prabha Kundur, *Power System Stability and Control*, EPRI, McGraw Hill, Inc., 1994.

[21] Ibid, Kundur.

[22] See Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing,"

Voltage controlled time-overcurrent and voltage-restrained time-overcurrent relays are excluded from this standard. When these relays are set based on equipment permissible overload capability, their operating times are much greater than 15 cycles for the current levels observed during a power swing.

Instantaneous overcurrent, time-overcurrent, and definite-time overcurrent relays with a time delay of less than 15 cycles for the current levels observed during a power swing are applicable and are required to be evaluated for identified Elements.

The generator loss-of-field protective function is provided by impedance relay(s) connected at the generator terminals. The settings are applied to protect the generator from a partial or complete loss of excitation under all generator loading conditions and, at the same time, be immune to tripping on stable power swings. It is more likely that the loss-of-field relay would operate during a power swing when the automatic voltage regulator (AVR) is in manual mode rather than when in automatic mode.[23] Figure 16 illustrates the loss-of-field relay in the R-X plot, which typically includes up to three zones of protection.

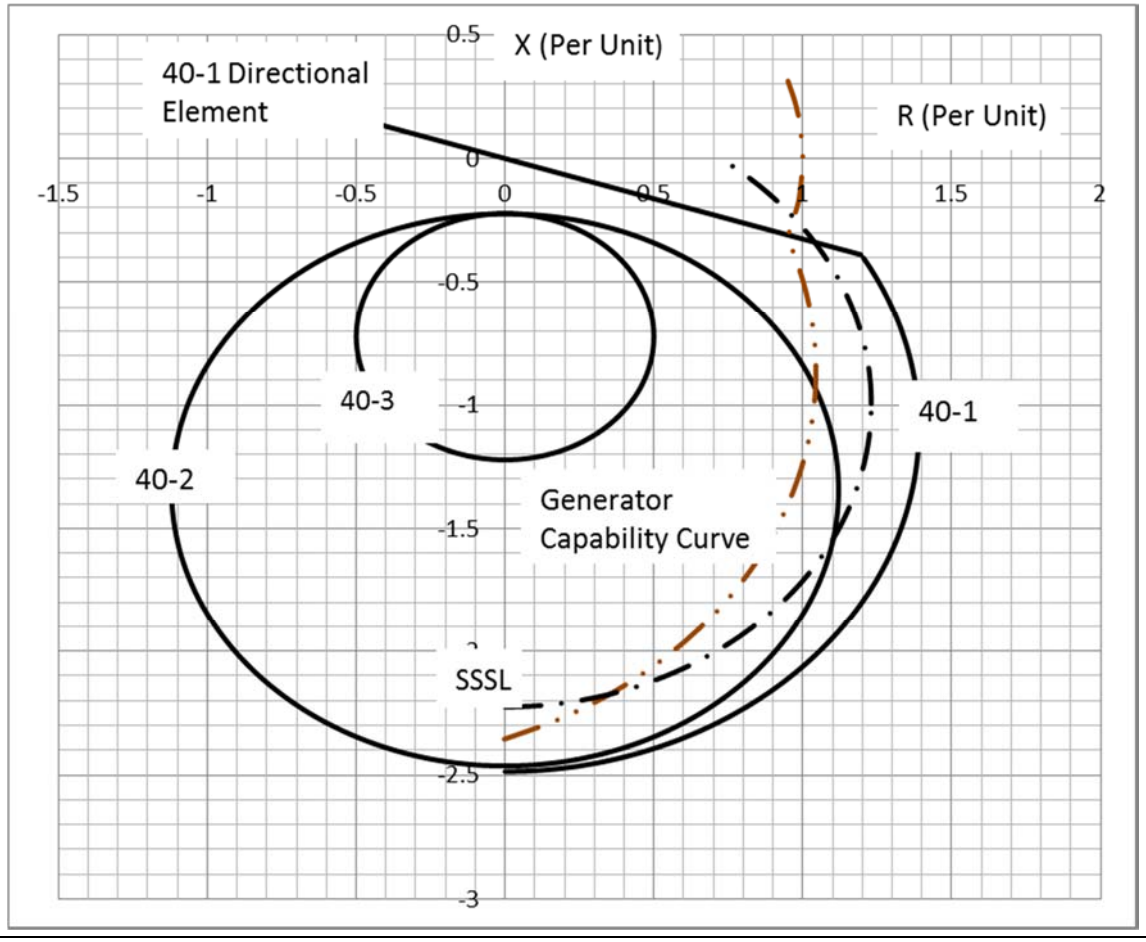


Figure 16: An R-X graph of typical impedance settings for loss-of-field relays.

[23] John Burdy, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

Loss-of-field characteristic 40-1 has a wider impedance characteristic (positive offset) than characteristic 40-2 or characteristic 40-3 and provides additional generator protection for a partial loss of field or a loss of field under low load (less than 10% of rated). The tripping logic of this protection scheme is established by a directional contact, a voltage setpoint, and a time delay. The voltage and time delay add security to the relay operation for stable power swings. Characteristic 40-3 is less sensitive to power swings than characteristic 40-2 and is set outside the generator capability curve in the leading direction. Regardless of the relay impedance setting, PRC-019[24] requires that the "in-service limiters operate before Protection Systems to avoid unnecessary trip" and "in-service Protection System devices are set to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits." Time delays for tripping associated with loss-of-field relays[25,26] have a range from 15 cycles for characteristic 40-2 to 60 cycles for characteristic 40-1 to minimize tripping during stable power swings. In PRC-026-1, 15 cycles establishes a threshold for applicability; however, it is the responsibility of the Generator Owner to establish settings that provide security against stable power swings and, at the same time, dependable protection for the generator.

The simple two-machine system circuit (method also used in the Application to Transmission Elements section) is used to analyze the effect of a power swing at a generator facility for load-responsive relays. In this section, the calculation method is used for calculating the impedance seen by the relay connected at a point in the circuit.[27] The electrical quantities used to determine the apparent impedance plot using this method are generator saturated transient reactance (X'_d), GSU transformer impedance (X_{GSU}), transmission line impedance (Z_L), and the system equivalent (Z_e) at the point of interconnection. All impedance values are known to the Generator Owner except for the system equivalent. The system equivalent is obtainable from the Transmission Owner. The sending-end and receiving-end source voltages are varied from 0.0 to 1.0 per unit to form the lens shape portion of the unstable power swing region. The voltage range of 0.7 to 1.0 results in a ratio range from 0.7 to 1.43. This ratio range is used to form the lower and upper loss-of-synchronism circle shapes of the unstable power swing region. A system separation angle of 120 degrees is used in accordance with PRC-026-1 – Attachment B criteria for each load-responsive protective relay evaluation.

Table 15 below is an example calculation of the apparent impedance locus method based on Figures 17 and 18.[28] In this example, the generator is connected to the 345 kV transmission system through the GSU transformer and has the listed ratings. Note that the load-responsive protective relays in this example may have ownership with the Generator Owner or the Transmission Owner.

---

[24] Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

[25] Ibid, Burdy.

[26] *Applied Protective Relaying*, Westinghouse Electric Corporation, 1979.

[27] Edward Wilson Kimbark, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

[28] Ibid, Kimbark.

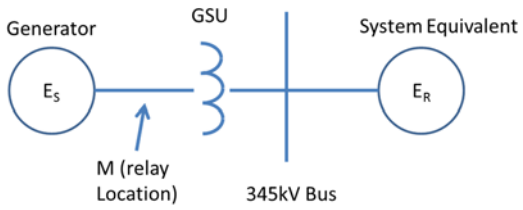


Figure 17: Simple one-line diagram of the system to be evaluated.

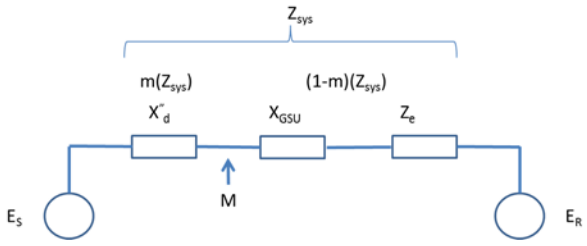


Figure 18: Simple system equivalent impedance diagram to be evaluated.[29]

Table15: Example Data (Generator)	
Input Descriptions	**Input Values**
Synchronous Generator nameplate (MVA)	940 MVA
Saturated transient reactance (940 MVA base)	$X'_d = 0.3845$ per unit
Generator rated voltage (Line-to-Line)	$20\ kV$
Generator step-up (GSU) transformer rating	$880\ MVA$
GSU transformer reactance (880 MVA base)	$X_{GSU} = 16.05\%$
System Equivalent (100 MVA base)	$Z_e = 0.00723\angle 90°$ per unit
Generator Owner Load-Responsive Protective Relays	
40-1	Positive Offset Impedance
	Offset = 0.294 per unit
	Diameter = 0.294 per unit
40-2	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 2.24 per unit
40-3	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 1.00 per unit
21-1	Diameter = 0.643 per unit
	MTA = 85°

[29] Ibid, Kimbark.

Table15: Example Data (Generator)	
50	I (pickup) = 5.0 per unit
Transmission Owned Load-Responsive Protective Relays	
21-2	Diameter = 0.55 per unit
	MTA = 85°

Calculations shown for a 120 degree angle and $E_S/E_R = 1$. The equation for calculating Z_R is:[30]

Eq. (106) $$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$$

Where m is the relay location as a function of the total impedance (real number less than 1)

E_S and E_R is the sending-end and receiving-end voltages

Z_{sys} is the total system impedance

Z_R is the complex impedance at the relay location and plotted on an R-X diagram

All of the above are constants (940 MVA base) while the angle δ is varied. Table 16 below contains calculations for a generator using the data listed in Table 15.

Table16: Example Calculations (Generator)			
The following calculations are on a 940 MVA base.			
Given:	$X'_d = j0.3845\ pu$	$X_{GSU} = j0.17144\ pu$	$Z_e = j0.06796\ pu$
Eq. (107)	$Z_{sys} = X'_d + X_{GSU} + Z_e$		
	$Z_{sys} = j0.3845\ pu + j0.17144\ pu + j0.06796\ pu$		
	$Z_{sys} = 0.6239\ \angle 90°\ pu$		
Eq. (108)	$m = \frac{X'_d}{Z_{sys}} = \frac{0.3845}{0.6239} = 0.6163$		
Eq. (109)	$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$		
	$Z_R = \left(\frac{(1-0.6163) \times (1\angle 120°) + (0.6163)(1\angle 0°)}{1\angle 120° - 1\angle 0°}\right) \times (0.6239\angle 90°)\ pu$		

[30] Ibid, Kimbark.

Table16: Example Calculations (Generator)	
	$Z_R = \left(\frac{0.4244 + j0.3323}{-1.5 + j\ 0.866}\right) \times (0.6239\angle 90°)\ pu$
	$Z_R = (0.3116 \angle -111.95°) \times (0.6239\angle 90°)\ pu$
	$Z_R = 0.194 \angle -21.95°\ pu$
	$Z_R = -0.18 - j0.073\ pu$

Table 17 lists the swing impedance values at other angles and at E_S/E_R = 1, 1.43, and 0.7. The impedance values are plotted on an R-X graph with the center being at the generator terminals for use in evaluating impedance relay settings.

Table 17: Sample Calculations for a Swing Impedance Chart for Varying Voltages at the Sending-End and Receiving-End.

	E_S/E_R=1		E_S/E_R=1.43		E_S/E_R=0.7	
	Z_R		Z_R		Z_R	
Angle (δ) (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)
90	0.320	-13.1	0.296	6.3	0.344	-31.5
120	0.194	-21.9	0.173	-0.4	0.227	-40.1
150	0.111	-41.0	0.082	-10.3	0.154	-58.4
210	0.111	-25.9	0.082	190.3	0.154	238.4
240	0.194	201.9	0.173	180.4	0.225	220.1
270	0.320	193.1	0.296	173.7	0.344	211.5

Requirement R2 Generator Examples

Distance Relay Application

Based on PRC-026-1 – Attachment B, Criterion A, the distance relay (21-1) (i.e., owned by the Generation Owner) characteristic is in the region where a stable power swing would not occur as shown in Figure 19. There is no further obligation to the owner in this standard for this load-responsive protective relay.

The distance relay (21-2) (i.e., owned by the Transmission Owner) is connected at the high-voltage side of the GSU transformer and its impedance characteristic is in the region where a stable power swing could occur causing the relay to operate. In this example, if the intentional time delay of this relay is less than 15 cycles, the PRC-026 – Attachment B, Criterion A cannot be met, thus the Transmission Owner is required to create a CAP (Requirement R3). Some of the options include,

but are not limited to, changing the relay setting (i.e., impedance reach, angle, time delay), modify the scheme (i.e., add PSB), or replace the Protection System. Note that the relay may be excluded from this standard if it has an intentional time delay equal to or greater than 15 cycles.

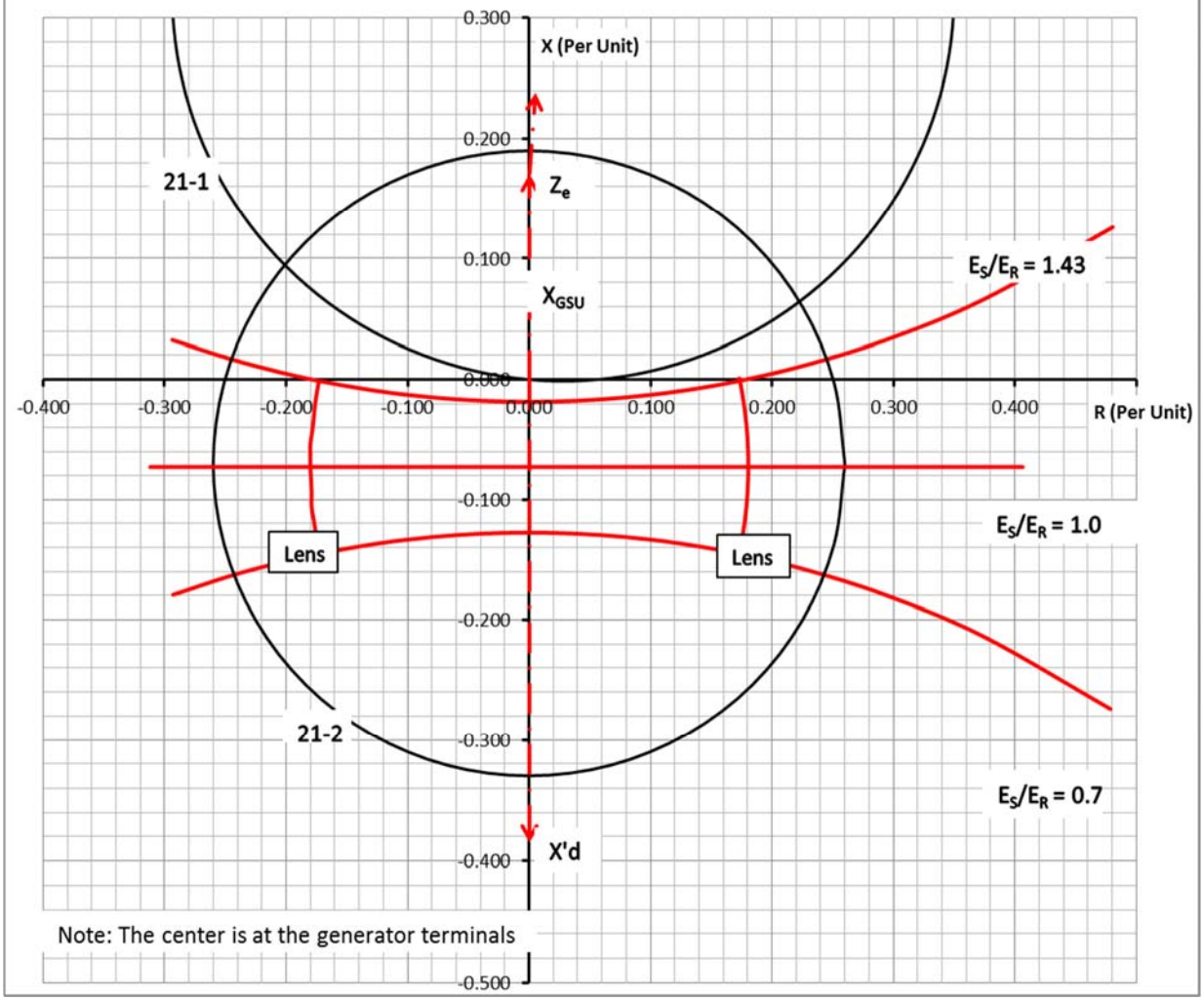


Figure 19: Swing impedance graph for impedance relays at a generating facility.

Loss-of-Field Relay Application

In Figure 20, the R-X diagram shows the loss-of-field relay (40-1 and 40-2) characteristics are in the region where a stable power swing can cause a relay operation. Protective relay 40-1 would be excluded if it has an intentional time delay equal to or greater than 15 cycles. Similarly, 40-2 would be excluded if its intentional time delay is equal to or greater than 15 cycles. For example, if 40-1 has a time delay of 1 second and 40-2 has a time delay of 0.25 seconds, they are excluded and there is no further obligation on the Generator Owner in this standard for these relays. The

loss-of-field relay characteristic 40-3 is entirely inside the unstable power swing region. In this case, the owner may select high speed tripping on operation of the 40-3 impedance element.

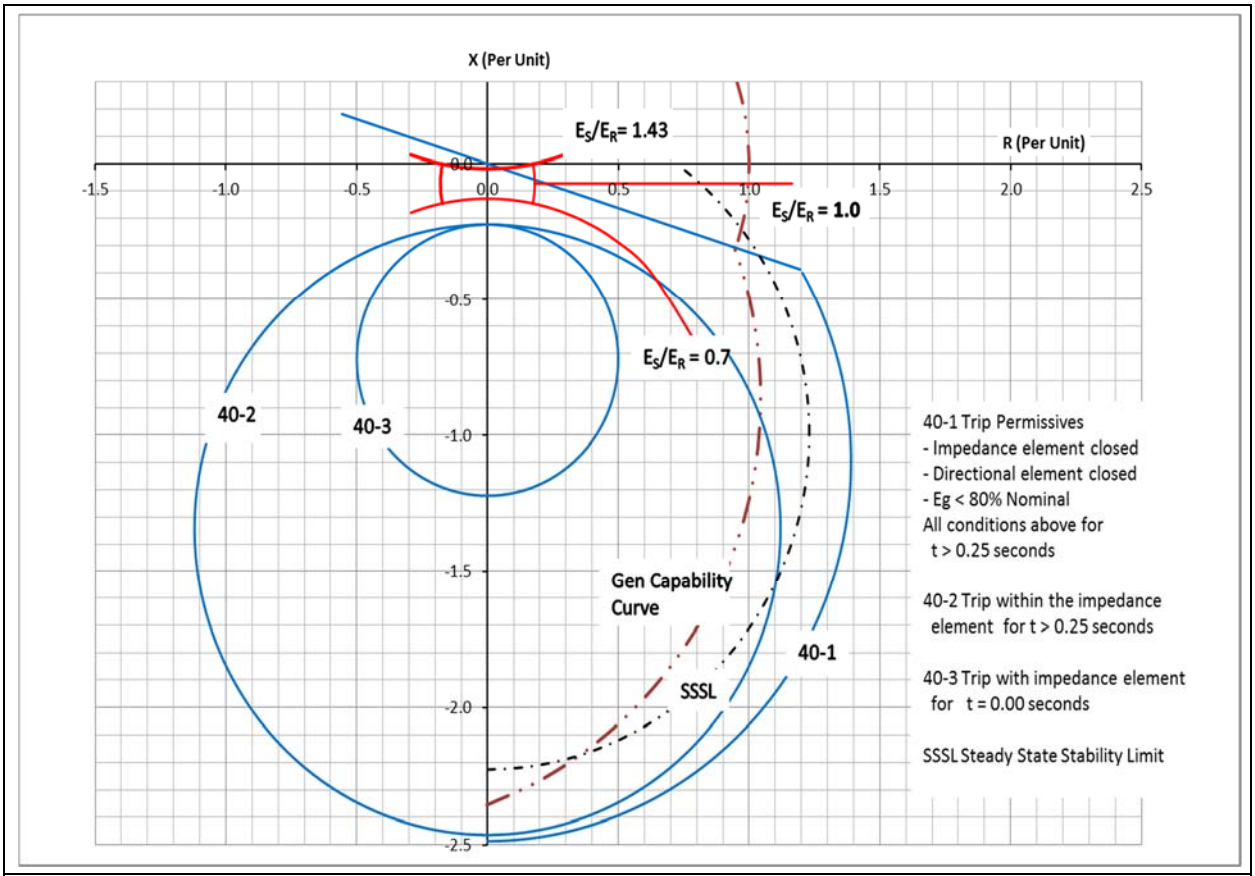


Figure 20: Typical R-X graph for loss-of-field relays with a portion of the unstable power swing region defined by PRC-026-1 – Attachment B, Criterion A.

Instantaneous Overcurrent Relay

In similar fashion to the transmission line overcurrent example calculation in Table 14, the instantaneous overcurrent relay minimum setting is established by PRC-026-1 – Attachment B, Criterion B. The solution is found by:

Eq. (110) $$I_{sys} = \frac{E_S - E_R}{Z_{\text{sys}}}$$

As stated in the relay settings in Table 15, the relay is installed on the high-voltage side of the GSU transformer with a pickup of 5.0 per unit. The maximum allowable current is calculated below.

$$I_{sys} = \frac{(1.05\angle 120° - 1.05\angle 0°)}{0.6239\angle 90°}\ pu$$

$$I_{sys} = \frac{1.819\angle 150°}{0.6239\angle 90°} pu$$

$$I_{sys} = 2.91\ \angle 60°\ pu$$

The instantaneous phase setting of 5.0 per unit is greater than the calculated system current of 2.91 per unit; therefore, it meets the PRC-026-1 – Attachment B, Criterion B.

Out-of-Step Tripping for Generation Facilities

Out-of-step protection for the generator generally falls into three different schemes. The first scheme is a distance relay connected at the high-voltage side of the GSU transformer with the directional element looking toward the generator. Because this relay setting may be the same setting used for generator backup protection (see Requirement R2 Generator Examples, Distance Relay Application), it is susceptible to tripping in response to stable power swings and would require modification. Because this scheme is susceptible to tripping in response to stable power swings and any modification to the mho circle will jeopardize the overall protection of the out-of-step protection of the generator, available technical literature does not recommend using this scheme specifically for generator out-of-step protection. The second and third out-of-step Protection System schemes are commonly referred to as single and double blinder schemes. These schemes are installed or enabled for out-of-step protection using a combination of blinders, a mho element, and timers. The combination of these protective relay functions provides out-of-step protection and discrimination logic for stable and unstable power swings. Single blinder schemes use logic that discriminate between stable and unstable power swings by issuing a trip command after the first slip cycle. Double blinder schemes are more complex than the single blinder scheme and, depending on the settings of the inner blinder, a trip for a stable power swing may occur. While the logic discriminates between stable and unstable power swings in either scheme, it is important that the trip initiating blinders be set at an angle greater than the stability limit of 120 degrees to remove the possibility of a trip for a stable power swing. Below is a discussion of the double blinder scheme.

Double Blinder Scheme

The double blinder scheme is a method for measuring the rate of change of positive sequence impedance for out-of-step swing detection. The scheme compares a timer setting to the actual elapsed time required by the impedance locus to pass between two impedance characteristics. In this case, the two impedance characteristics are simple blinders, each set to a specific resistive reach on the R-X plane. Typically, the two blinders on the left half plane are the mirror images of those on the right half plane. The scheme typically includes a mho characteristic which acts as a starting element, but is not a tripping element.

The scheme detects the blinder crossings and time delays as represented on the R-X plane as shown in Figure 21. The system impedance is composed of the generator transient (X_d'), GSU transformer (X_T), and transmission system (X_{system}), impedances.

The scheme logic is initiated when the swing locus crosses the outer Blinder R1 (Figure 21), on the right at separation angle α. The scheme only commits to take action when a swing crosses the

inner blinder. At this point the scheme logic seals in the out-of-step trip logic at separation angle β. Tripping actually asserts as the impedance locus leaves the scheme characteristic at separation angle δ.

The power swing may leave both inner and outer blinders in either direction, and tripping will assert. Therefore, the inner blinder must be set such that the separation angle β is large enough that the system cannot recover. This angle should be set at 120 degrees or more. Setting the angle greater than 120 degrees satisfies the PRC-026-1 – Attachment B, Criterion A (No. 1, 1st bullet) since the tripping function is asserted by the blinder element. Transient stability studies may indicate that a smaller stability limit angle is acceptable under PRC-026-1 – Attachment B, Criterion A (No. 1, 2nd bullet). In this respect, the double blinder scheme is similar to the double lens and triple lens schemes and many transmission application out-of-step schemes.

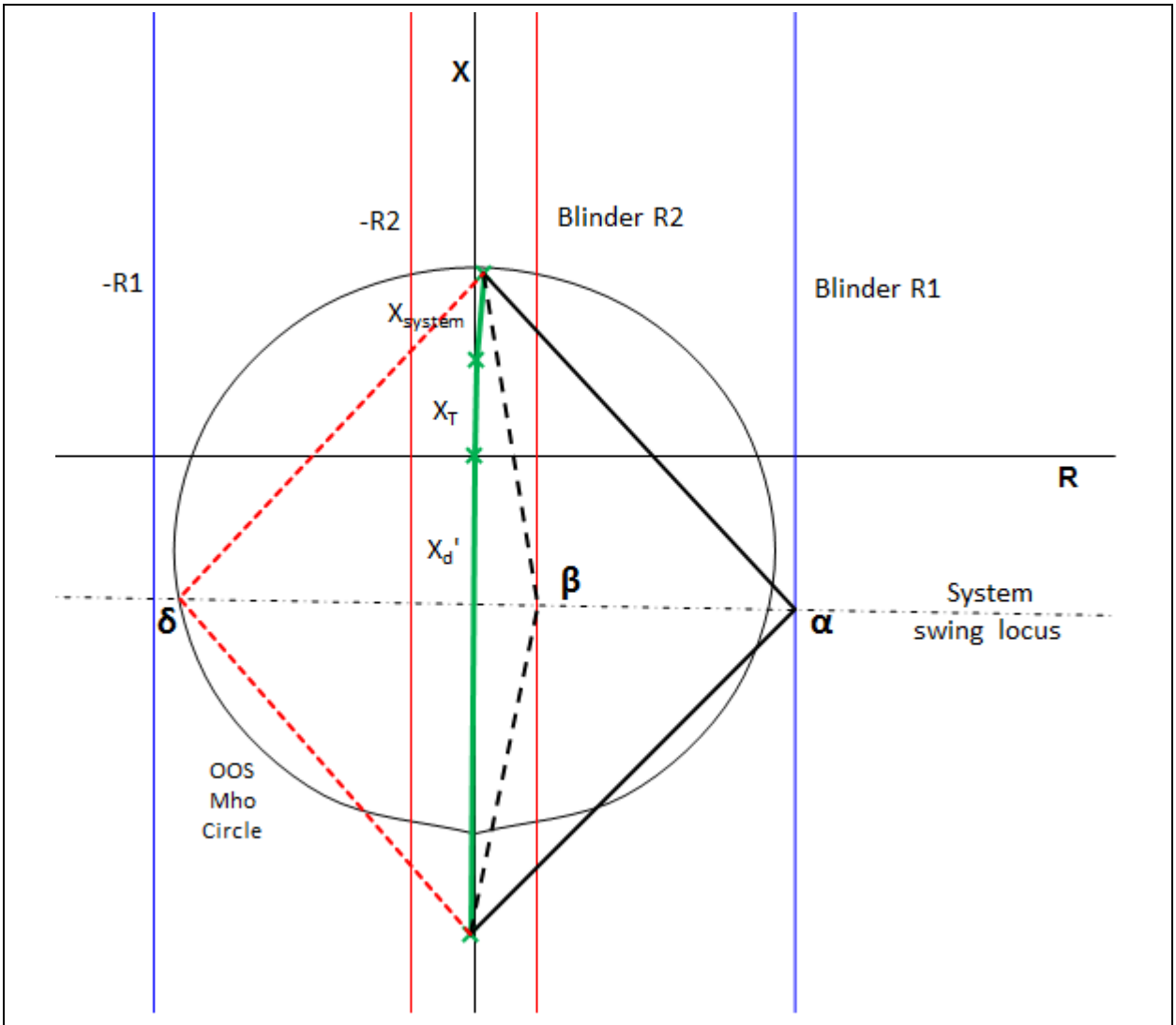


Figure 21: Double Blinder Scheme generic out of step characteristics.

Figure 22 illustrates a sample setting of the double blinder scheme for the example 940 MVA generator. The only setting requirement for this relay scheme is the right inner blinder, which must be set greater than the separation angle of 120 degrees (or a lesser angle based on a transient stability study) to ensure that the out-of-step protective function is expected to not trip in response to a stable power swing during non-Fault conditions. Other settings such as the mho characteristic, outer blinders, and timers are set according to transient stability studies and are not a part of this standard.

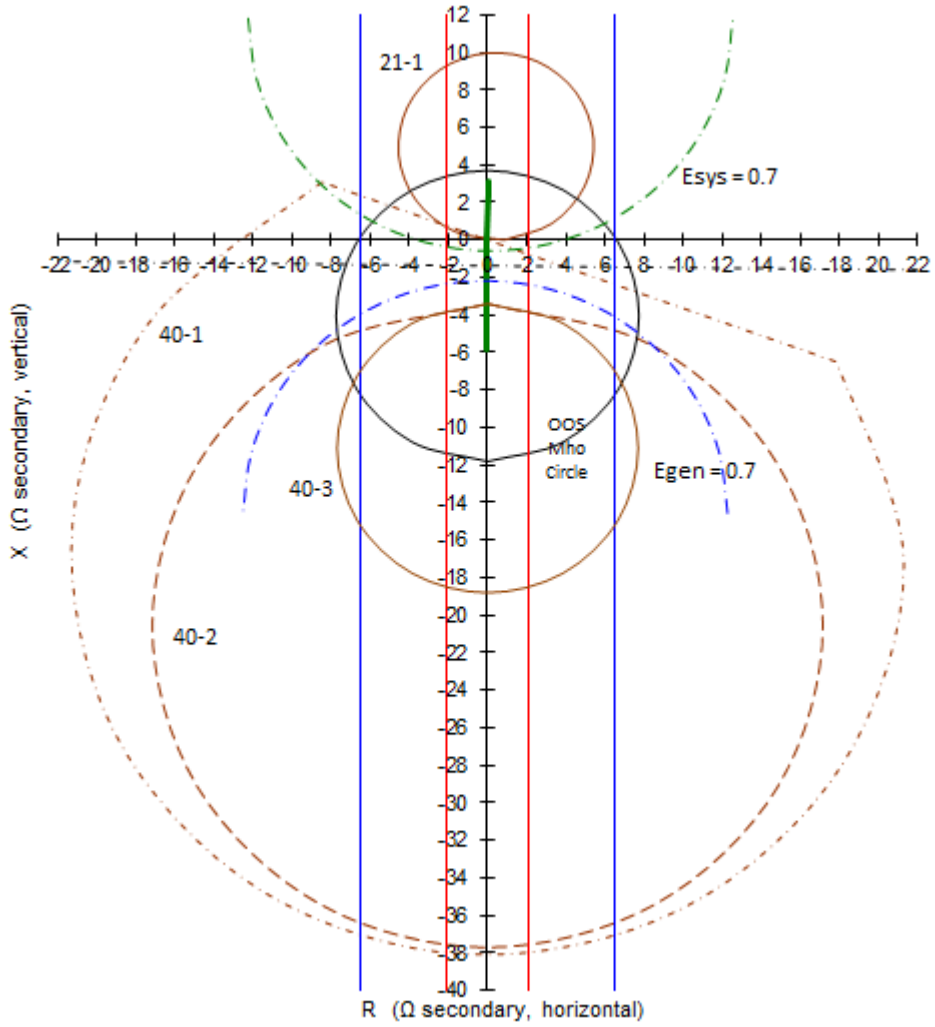


Figure 22: Double Blinder Out-of-Step Scheme with unit impedance data and load-responsive protective relay impedance characteristics for the example 940 MVA generator, scaled in relay secondary ohms.

Requirement R3

To achieve the stated purpose of this standard, which is to ensure that relays are expected to not trip in response to stable power swings during non-Fault conditions, this Requirement ensures that the applicable entity develops a Corrective Action Plan (CAP) that reduces the risk of relays tripping in response to a stable power swing during non-Fault conditions that may occur on any applicable BES Element.

Requirement R4

To achieve the stated purpose of this standard, which is to ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions, the applicable entity is required to implement any CAP developed pursuant to Requirement R3 such that the Protection System will meet PRC-026-1 – Attachment B criteria or can be excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element). Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until all actions are complete. Accomplishing this objective is intended to reduce the occurrence of Protection System tripping during a stable power swing, thereby improving reliability and minimizing risk to the BES.

The following are examples of actions taken to complete CAPs for a relay that did not meet PRC-026-1 – Attachment B and could be at-risk of tripping in response to a stable power swing during non-Fault conditions. A Protection System change was determined to be acceptable (without diminishing the ability of the relay to protect for faults within its zone of protection).

> **Example R4a:** Actions: Settings were issued on 6/02/2015 to reduce the Zone 2 reach of the impedance relay used in the directional comparison unblocking (DCUB) scheme from 30 ohms to 25 ohms so that the relay characteristic is completely contained within the lens characteristic identified by the criterion. The settings were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.
>
> **Example R4b:** Actions: Settings were issued on 6/02/2015 to enable out-of-step blocking on the existing microprocessor-based relay to prevent tripping in response to stable power swings. The setting changes were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.

The following is an example of actions taken to complete a CAP for a relay responding to a stable power swing that required the addition of an electromechanical power swing blocking relay.

> **Example R4c:** Actions: A project for the addition of an electromechanical power swing blocking relay to supervise the Zone 2 impedance relay was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The relay installation was completed on 9/25/2015. CAP was completed on 9/25/2015.

The following is an example of actions taken to complete a CAP with a timetable that required updating for the replacement of the relay.

> **Example R4d:** Actions: A project for the replacement of the impedance relays at both terminals of line X with line current differential relays was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The completion of the project was postponed due to line outage rescheduling from 11/15/2015 to 3/15/2016. Following the timetable change, the impedance relay replacement was completed on 3/18/2016. CAP was completed on 3/18/2016.

The CAP is complete when all the documented actions to remedy the specific problem (i.e., unnecessary tripping during stable power swings) are completed.

Justification for Including Unstable Power Swings in the Requirements

Protection Systems that are applicable to the Standard and must be secure for a stable power swing condition (i.e., meets PRC-026-1 – Attachment B criteria) are identified based on Elements that are susceptible to both stable and unstable power swings. This section provides an example of why Elements that trip in response to unstable power swings (in addition to stable power swings) are identified and that their load-responsive protective relays need to be evaluated under PRC-026-1 – Attachment B criteria.

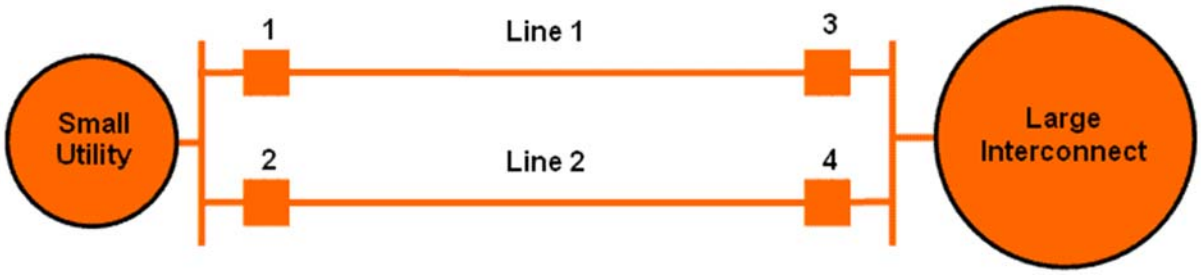


Figure 23: A simple electrical system where two lines tie a small utility to a much larger interconnection.

In Figure 23 the relays at circuit breakers 1, 2, 3, and 4 are equipped with a typical overreaching Zone 2 pilot system, using a Directional Comparison Blocking (DCB) scheme. Internal faults (or power swings) will result in instantaneous tripping of the Zone 2 relays if the measured fault or power swing impedance falls within the zone 2 operating characteristic. These lines will trip on

pilot Zone 2 for out-of-step conditions if the power swing impedance characteristic enters into Zone 2. All breakers are rated for out-of-phase switching.

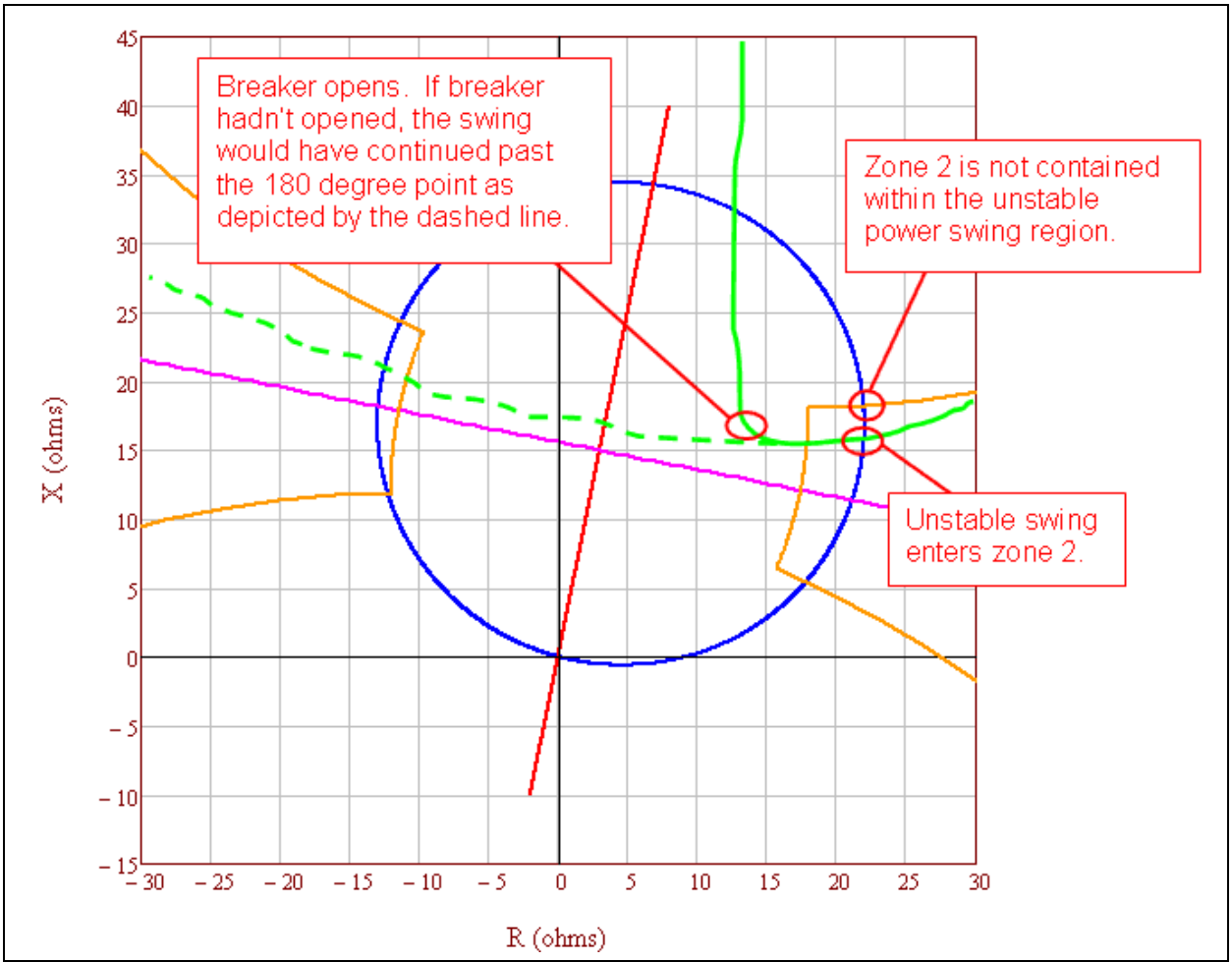


Figure 24: In this case, the Zone 2 element on circuit breakers 1, 2, 3, and 4 did not meet the PRC-026-1 – Attachment B criteria (this figure depicts the power swing as seen by relays on breakers 3 and 4).

In Figure 24, a large disturbance occurs within the small utility and its system goes out-of-step with the large interconnect. The small utility is importing power at the time of the disturbance. The actual power swing, as shown by the solid green line, enters the Zone 2 relay characteristic on the terminals of Lines 1, 2, 3, and 4 causing both lines to trip as shown in Figure 25.

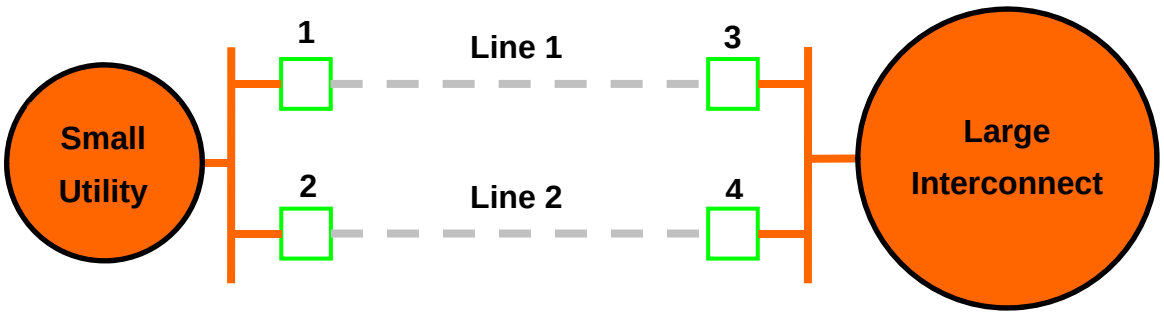


Figure 25: Islanding of the small utility due to Lines 1 and 2 tripping in response to an unstable power swing.

In Figure 25, the relays at circuit breakers 1, 2, 3, and 4 have correctly tripped due to the unstable power swing (shown by the dashed green line in Figure 24), de-energizing Lines 1 and 2, and creating an island between the small utility and the big interconnect. The small utility shed 500 MW of load on underfrequency and maintained a load to generation balance.

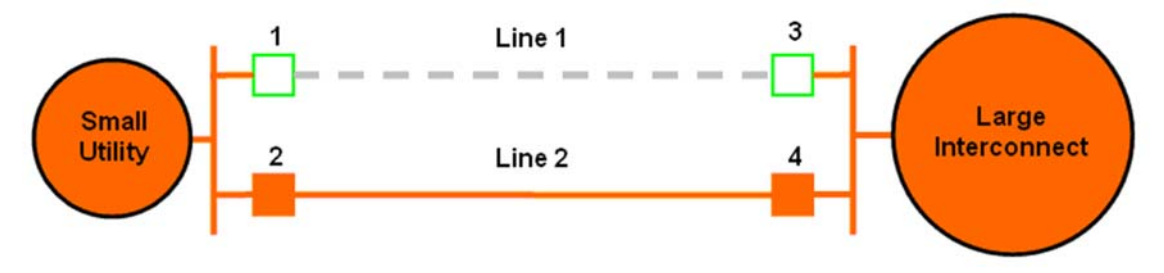


Figure 26: Line 1 is out-of-service for maintenance, Line 2 is loaded beyond its normal rating (but within its emergency rating).

Subsequent to the correct tripping of Lines 1 and 2 for the unstable power swing in Figure 25, another system disturbance occurs while the system is operating with Line 1 out-of-service for maintenance. The disturbance causes a stable power swing on Line 2, which challenges the relays at circuit breakers 2 and 4 as shown in Figure 27.

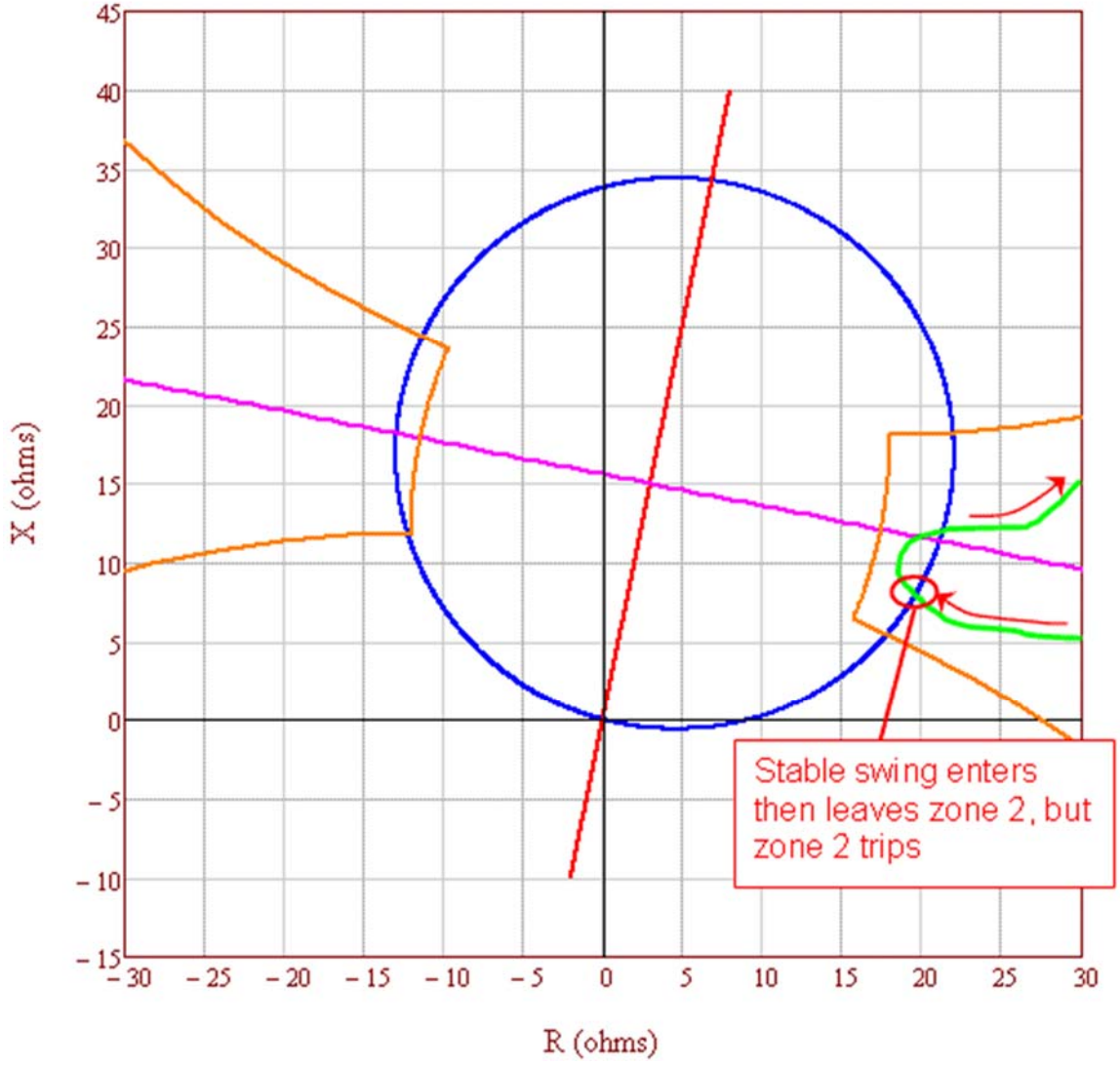


Figure 27: Relays on circuit breakers 2 and 4 were not addressed to meet the PRC-026-1 – Attachment B criteria following the previous unstable power swing event.

If the relays on circuit breakers 2 and 4 were not addressed under the Requirements for the previous unstable power swing condition, the relays would trip in response to the stable power swing, which would result in unnecessary system separation, load shedding, and possibly cascading or blackout.

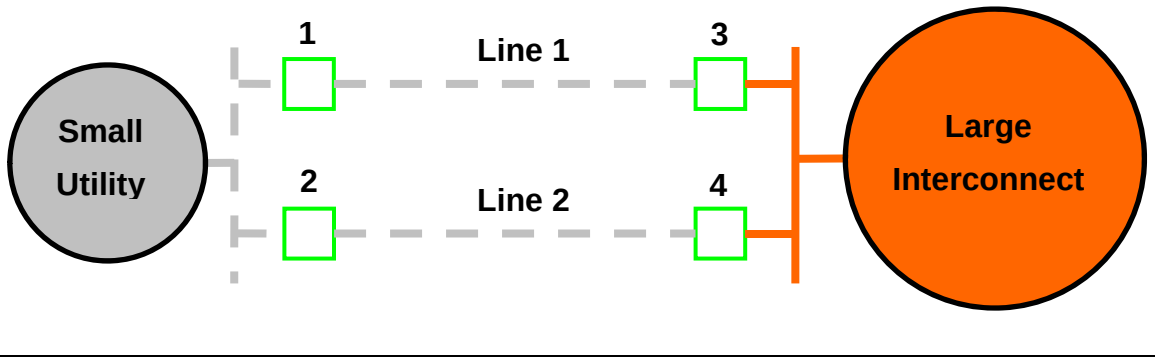


Figure 28: Possible blackout of the small utility.

If the relays that tripped in response to the previous unstable power swing condition in Figure 24 were addressed under the Requirements to meet PRC-026-1 - Attachment B criteria, the unnecessary tripping of the relays for the stable power swing shown in Figure 28 would have been averted, and the possible blackout of the small utility would have been avoided.

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 Planning Coordinator has a wide-area view and is in the position to identify generator, transformer, and transmission line BES Elements which meet the criteria, if any. The criteria-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document *Protection System Response to Power Swings*, August 2013 ("PSRPS Report"),[31] which recommends a focused approach to determine an at-risk BES Element. See the Guidelines and Technical Basis for a detailed discussion of the criteria.

Rationale for R2

The Generator Owner and Transmission Owner are in a position to determine whether their load-responsive protective relays meet the PRC-026-1 – Attachment B criteria. Generator, transformer, and transmission line BES Elements are identified by the Planning Coordinator in Requirement R1 and by the Generator Owner and Transmission Owner following an actual event where the Generator Owner and Transmission Owner became aware (i.e., through an event analysis or

[31] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

Protection System review) tripping was due to a stable or unstable power swing. A period of 12 calendar months allows sufficient time for the entity to conduct the evaluation.

Rationale for R3

To meet the reliability purpose of the standard, a CAP is necessary to ensure the entity's Protection System meets the PRC-026-1 – Attachment B criteria (1st bullet) so that protective relays are expected to not trip in response to stable power swings. A CAP may also be developed to modify the Protection System for exclusion under PRC-026-1 – Attachment A (2nd bullet). Such an exclusion will allow the Protection System to be exempt from the Requirement for future events. The phrase, "…while maintaining dependable fault detection and dependable out-of-step tripping…" in Requirement R3 describes that the entity is to comply with this standard, while achieving their desired protection goals. Refer to the Guidelines and Technical Basis, Introduction, for more information.

Rationale for R4

Implementation of the CAP must accomplish all identified actions to be complete to achieve the desired reliability goal. During the course of implementing a CAP, updates may be necessary for a variety of reasons such as new information, scheduling conflicts, or resource issues. Documenting CAP changes and completion of activities provides measurable progress and confirmation of completion.

Rationale for Attachment B (Criterion A)

The PRC-026-1 – Attachment B, Criterion A provides a basis for determining if the relays are expected to not trip for a stable power swing having a system separation angle of up to 120 degrees with the sending-end and receiving-end voltages varying from 0.7 to 1.0 per unit (See Guidelines and Technical Basis).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2015-09 Establish and Communicate System Operating Limits

Applicable Standard(s) and Definitions

- FAC-011-4 System Operating Limits Methodology for the Operations Horizon
- FAC-014-3 Establish and Communicate System Operating Limits
- FAC-015-1 Coordination of Planning Assessments with the Reliability Coordinator's SOL Methodology
- CIP-014-3 Physical Security
- FAC-003-5 Transmission Vegetation Management
- FAC-013-3 Assessment of Transfer Capability for the Near-term Transmission Planning Horizon
- PRC-002-3 Disturbance Monitoring and Reporting Requirements
- PRC-023-5 Transmission Relay Loadability
- PRC-026-2 Relay Performance During Stable Power Swings
- Definition of System Voltage Limit in the Glossary of Terms Used in NERC Reliability Standards ("NERC Glossary")
- Definition of System Operating Limit in the NERC Glossary

Requested Retirement(s)

- FAC-010-3 System Operating Limits Methodology for the Planning Horizon
- FAC-011-3 System Operating Limits Methodology for the Operations Horizon
- FAC-014-2 Establish and Communicate System Operating Limits
- CIP-014-2 Physical Security
- FAC-003-4 Transmission Vegetation Management
- FAC-013-2 Assessment of Transfer Capability for the Near-term Transmission Planning Horizon
- PRC-002-2 Disturbance Monitoring and Reporting Requirements
- PRC-023-4 Transmission Relay Loadability
- PRC-026-1 Relay Performance During Stable Power Swings
- Currently-effective definition of System Operating Limit

Prerequisite Approvals

In addition to approval of the Reliability Standards included in this implementation plan, retirement of Reliability Standard FAC-010-3 cannot occur until the modifications in Reliability Standard CIP-002-6 (Cyber Security – BES Cyber System Categorization), Attachment 1, Criteria 2.6 and 2.9 become effective.

General Considerations

The elements of the Implementation Plans for PRC-002-2, PRC-023-4, and PRC-005-3 listed below shall remain applicable to PRC-002-3. PRC-023-5, and PRC-026-2and are incorporated herein by reference.

- Implementation of PRC-002-2 Requirements R2, R3, R4, R6, R7, R8, R9, R10, R11:
  - Entities shall be at least 50 percent compliant within four (4) years of the effective date of PRC-002-2 and fully compliant within six (6) years of the effective date.
  - Entities that own only one (1) identified BES bus, BES Element, or generating unit shall be fully compliant within six (6) years of the effective date.
- Implementation of Newly Classified Remedial Action Schemes (RAS) (PRC-023-4)
  - Entities with newly classified "Remedial Action Scheme" (RAS) resulting from the application of the revised definition must be fully compliant with all Reliability Standards applicable RAS twenty-four (24) months from the Effective Date of the revised definition of RAS. This additional time applies only to existing schemes that must transition to RAS due to the revised definition. The additional time does not apply to future RAS that may be created following implementation of the revised definition.
- Implementation of PRC-026-1
  - Requirement R1: First day of the first full calendar year that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.
  - Requirements R2, R3, and R4: First day of the first full calendar year that is 36 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 36 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Effective Date

The effective date for proposed Reliability Standards FAC-011-4, FAC-014-3, FAC-015-1, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, and the NERC Glossary terms "System Voltage Limit" and System Operating Limit" is provided below:

Where approval by an applicable governmental authority is required, Reliability Standards FAC-011-4, FAC-014-3, FAC-015-1, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, and the NERC Glossary terms "System Voltage Limit" and "System Operating Limit" shall become effective the first day of the first calendar quarter that is twelve (12) calendar months after the

effective date of the applicable governmental authority's order approving the standards and terms, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standards FAC-011-4, FAC-014-3, FAC-015-1, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, the NERC Glossary terms "System Voltage Limit" and "System Operating Limit" shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the date the standards and terms are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

Currently-Effective NERC Reliability Standards

Reliability Standards FAC-010-3, FAC-011-3, FAC-014-2, CIP-014-2, FAC-003-4, FAC-013-2, PRC-002-2, PRC-023-4, and PRC-026-1 shall be retired immediately prior to the effective date of the proposed Reliability Standards FAC-011-4, FAC-014-3, FAC-015, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, and the current definition of System Operating Limit.

Initial Performance of Periodic Requirements

FAC-014-3 Requirement R5, Parts 5.1 and 5.2

The initial performance of FAC-014-3, Requirement R5, Parts 5.1 and 5.2 must be within 12 calendar months of the effective date of FAC-014-3.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2015-09 Establish and Communicate System Operating Limits

Applicable Standard(s) and Definitions

- ~~Definition of System Voltage Limit (SVL) in the Glossary of Terms Used in NERC Reliability Standards ("NERC Glossary")~~
  - FAC-011-4 System Operating Limits Methodology for the Operations Horizon
  - FAC-014-3 Establish and Communicate System Operating Limits
  - FAC-015-1 Coordination of Planning Assessments with the Reliability Coordinator's SOL Methodology
- CIP-014-3 Physical Security
- FAC-003-5 Transmission Vegetation Management
- FAC-013-3 Assessment of Transfer Capability for the Near-term Transmission Planning Horizon
- PRC-002-3 Disturbance Monitoring and Reporting Requirements
- PRC-023-5 Transmission Relay Loadability
- PRC-026-2 Relay Performance During Stable Power Swings
- Definition of System Voltage Limit in the Glossary of Terms Used in NERC Reliability Standards ("NERC Glossary")
- Definition of System Operating Limit in the NERC Glossary

Requested Retirement(s)

- FAC-010-3 System Operating Limits Methodology for the Planning Horizon
- FAC-011-3 System Operating Limits Methodology for the Operations Horizon
- FAC-014-2 Establish and Communicate System Operating Limits

~~[*New/Modified/Retired*] Terms in the NERC Glossary of Terms~~

~~**Proposed New Definition(s):**~~
~~System Voltage Limit: The maximum and minimum steady-state voltage limits (both normal and emergency) that provide for acceptable System performance.~~

~~Applicable Entities~~

- ~~Reliability Coordinator~~
- ~~Planning Coordinator~~
- CIP-014-2 Physical Security
- FAC-003-4 Transmission ~~Planner~~Vegetation Management
- FAC-013-2 Assessment of Transfer Capability for the Near-term Transmission ~~Operator~~Planning Horizon
- PRC-002-2 Disturbance Monitoring and Reporting Requirements

- PRC-023-4 Transmission Relay Loadability
- PRC-026-1 Relay Performance During Stable Power Swings
- Currently-effective definition of System Operating Limit

Prerequisite Approvals

In addition to approval of the Reliability Standards included in this implementation plan, retirement of Reliability Standard FAC-010-3 cannot occur until the modifications in Reliability Standard CIP-002-6 (Cyber Security – BES Cyber System Categorization), Attachment 1, Criteria 2.6 and 2.9 become effective.

General Considerations

The elements of the Implementation Plans for PRC-002-2, PRC-023-4, and PRC-005-3 listed below shall remain applicable to PRC-002-3. PRC-023-5, and PRC-026-2and are incorporated herein by reference.

- Implementation of PRC-002-2 Requirements R2, R3, R4, R6, R7, R8, R9, R10, R11:
  - Entities shall be at least 50 percent compliant within four (4) years of the effective date of PRC-002-2 and fully compliant within six (6) years of the effective date.
  - Entities that own only one (1) identified BES bus, BES Element, or generating unit shall be fully compliant within six (6) years of the effective date.
- Implementation of Newly Classified Remedial Action Schemes (RAS) (PRC-023-4)
  - Entities with newly classified “Remedial Action Scheme” (RAS) resulting from the application of the revised definition must be fully compliant with all Reliability Standards applicable RAS twenty-four (24) months from the Effective Date of the revised definition of RAS. This additional time applies only to existing schemes that must transition to RAS due to the revised definition. The additional time does not apply to future RAS that may be created following implementation of the revised definition.
- Implementation of PRC-026-1
  - Requirement R1: First day of the first full calendar year that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.
  - Requirements R2, R3, and R4: First day of the first full calendar year that is 36 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first full calendar year that is 36 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Effective Date

The effective date for proposed Reliability Standards FAC-011-4, FAC-014-3, ~~and~~ FAC-015-1~~ and~~, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, and the NERC Glossary ~~term~~terms "System Voltage Limit" and System Operating Limit" is provided below:

Where approval by an applicable governmental authority is required, Reliability Standards FAC-011-4, FAC-014-3, ~~and~~ FAC-015-1, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, and the NERC Glossary ~~term~~terms "System Voltage Limit" and "System Operating Limit" shall become effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standards and ~~term~~terms, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standards FAC-011-4, FAC-014-3, ~~and~~ FAC-015-1~~ and~~, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, the NERC Glossary ~~term~~terms "System Voltage Limit" and "System Operating Limit" shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the date the standards and ~~term~~terms are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

Currently-Effective NERC Reliability Standards

Reliability Standards FAC-010-3, FAC-011-3, ~~and FAC-014-2~~FAC-014-2, CIP-014-2, FAC-003-4, FAC-013-2, PRC-002-2, PRC-023-4, and PRC-026-1 shall be retired immediately prior to the effective date of the proposed Reliability Standards FAC-011-4, FAC-014-3, ~~and FAC-015.~~FAC-015, CIP-014-3, FAC-003-5, FAC-013-3, PRC-002-3, PRC-023-5, PRC-026-2, and the current definition of System Operating Limit.

Initial Performance of Periodic Requirements

FAC-014-3 Requirement R5, Parts 5.1 and 5.2

The initial performance of FAC-014-3, Requirement R5, Parts 5.1 and 5.2 must be within 12 calendar months of the effective date of FAC-014-3.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard 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
45-day formal comment period with ballot	09/29/17 – 11/14/17

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2018 – October 2018
10-day final ballot	October 2018
NERC Board adoption	November 2018

A. Introduction

1. **Title:** Coordination of Planning Assessments with the Reliability Coordinator's SOL Methodology

2. **Number:** FAC-015-1

3. **Purpose:** To ensure the Facility Ratings, System steady-state voltage limits, and stability criteria used in Planning Assessments are coordinated with the Reliability Coordinator's System Operating Limits (SOL) Methodology.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator

   4.1.2. Transmission Planner

5. **Effective Date:** See Implementation Plan for Project 2015-09.

B. Requirements and Measures

R1. Each Planning Coordinator and each of its Transmission Planners, when developing its steady-state modeling data requirements, shall implement a process to ensure that Facility Ratings used in its Planning Assessment of the Near-Term Transmission Planning Horizon are equally limiting or more limiting than the owner-provided Facility Ratings used in operations per the Reliability Coordinator's SOL Methodology. The process may allow the use of less limiting Facility Ratings if: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- The Facility has higher Facility Ratings as a result of a planned upgrade, addition, or Corrective Action Plan;
- Facility Rating differences are due to variations in ambient temperature assumptions;
- The Planning Coordinator provided a technical rationale for using a less limiting Facility Rating to each affected Transmission Planner and Reliability Coordinator; or
- The Transmission Planner provided a technical rationale for using a less limiting Facility Rating to each affected Planning Coordinator and Reliability Coordinator.

M1. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator implemented its process in accordance with Requirement R1.

R2. Each Planning Coordinator and each of its Transmission Planners shall implement a process to ensure that System steady-state voltage limits used in its Planning

Assessment of the Near-Term Transmission Planning Horizon are equally limiting or more limiting than the System Voltage Limits used in operations per the Reliability Coordinator's SOL Methodology. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- The Planning Coordinator may use less limiting System Voltage Limits if it provides a technical rationale for using less limiting System Voltage Limits to each affected Transmission Planner and Reliability Coordinator.
- The Transmission Planner may use less limiting System Voltage Limits if it provides a technical rationale for using less limiting System Voltage Limits to each affected Planning Coordinator and Reliability Coordinator.

M2. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator implemented its process in accordance with Requirement R2.

R3. Each Planning Coordinator and each of its Transmission Planners shall implement a process to ensure the stability performance criteria used in its Planning Assessment of the Near-Term Transmission Planning Horizon are equally limiting or more limiting than the stability performance criteria used in operations per the Reliability Coordinator's SOL Methodology. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- The Planning Coordinator may use less limiting stability performance criteria if it provides a technical rationale for using less limiting stability performance criteria to each affected Transmission Planner and Reliability Coordinator.
- The Transmission Planner may use less limiting stability performance criteria if it provides a technical rationale for using less limiting stability performance criteria to each affected Planning Coordinator and Reliability Coordinator.

M3. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator implemented its process in accordance with Requirement R3.

R4. Each Planning Coordinator and each Transmission Planner shall communicate any instability, Cascading or uncontrolled separation identified in either its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability assessment (Planning Coordinator only) to each impacted Reliability Coordinator, Transmission Operator, Transmission Owner, and Generation Owner. This communication shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

4.1 The type of instability identified (e.g., voltage collapse, angular instability, transient voltage dip criteria violation);

4.2 The associated stability criteria used as part of determining the instability;

4.3 The associated Contingency(ies) and any Facilities critical to the instability, Cascading or uncontrolled separation;

4.4 A description of the studied System conditions when the instability, Cascading or uncontrolled separation was identified;

4.5 Any Remedial Action Scheme action, undervoltage load shedding (UVLS) action, underfrequency load shedding (UFLS) action, interruption of Firm Transmission Service, or Non-Consequential Load Loss required to address the instability, Cascading or uncontrolled separation; and

4.6 Any Corrective Action Plan associated with the instability, Cascading or uncontrolled separation.

M4. 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 R4.

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 Planning Coordinator and Transmission Planner shall keep evidence for Requirements R1 through R4 for the most current year plus the previous three years.

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	The Planning Coordinator or a Transmission Planner used less limiting Facility Ratings than the Facility Ratings established in accordance with its Reliability Coordinator's SOL Methodology, but failed to identify the exclusion criteria allowing the use of less limiting Facility Ratings.	The Planning Coordinator or a Transmission Planner failed to implement a process to ensure that Facility Ratings used in Planning Assessment are equally limiting or more limiting than those established in its Reliability Coordinator's SOL Methodology.
R2.	N/A	N/A	The Planning Coordinator or a Transmission Planner used less limiting System steady-state voltage limits than the System Voltage Limits established in accordance with its Reliability Coordinator's SOL Methodology, but did not provide its technical rationale.	The Planning Coordinator or a Transmission Planner failed to implement a process to ensure that System steady-state voltage limits used in Planning Assessments are equally limiting or more limiting than the System Voltage Limits established in accordance with its Reliability Coordinator's SOL Methodology.

R3.	N/A	N/A	The Planning Coordinator or a Transmission Planner used less limiting stability performance criteria than the stability performance criteria established in its Reliability Coordinator's SOL Methodology, but did not provide its technical rationale.	The Planning Coordinator or a Transmission Planner failed to implement a process to ensure that stability performance criteria used in Planning Assessments are equally limiting or more limiting than the stability performance criteria established in the Reliability Coordinator's SOL Methodology.
R4.	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain one of the elements listed in Requirement R4, Parts 4.1 – 4.6.	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain two of the elements listed in Requirement R4, Parts 4.1 – 4.6.	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain three elements listed in Requirement R4, Parts 4.1 – 4.6.	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain four or more of the elements listed in Requirement R4, Parts 4.1 – 4.6. OR

				The Planning Coordinator failed to communicate any identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator, Transmission Operator, Transmission Owner and Generator Owner.

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

Implementation Plan

Version History

Version	Date	Action	Change Tracking
1		Project 2015-09 SOL – Adopt new standard.	New

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
45-day formal comment period with ballot	09/29/17 – 11/14/17

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~September 2017 – November 2017~~
45-day formal comment period with additional ballot	~~January~~August 2018 – ~~February~~October 2018
10-day final ballot	~~February~~October 2018
NERC Board adoption	~~May~~November 2018

A. Introduction

1. **Title:** Coordination of Planning Assessments with the Reliability Coordinator's SOL Methodology

2. **Number:** FAC-015-1

3. **Purpose:** To ensure the Facility Ratings, System steady-state voltage limits, and stability criteria used in Planning Assessments are coordinated with the Reliability Coordinator's System Operating Limits (SOL) Methodology.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator

   4.1.2. Transmission Planner

5. **Effective Date:** See Implementation Plan for Project 2015-09.

B. Requirements and Measures

R1. Each Planning Coordinator and each of its Transmission Planners, when developing its steady-state modeling data requirements, shall implement a process to ensure that Facility Ratings used in its Planning Assessment of the Near-Term Transmission Planning Horizon are equally limiting or more limiting than ~~those established~~the owner-provided Facility Ratings used in ~~accordance with its~~ operations per the Reliability Coordinator's SOL Methodology. ~~If~~ The process may allow the ~~Planning Coordinator uses~~use of less limiting Facility Ratings ~~than the Facility Ratings established in accordance with its Reliability Coordinator's SOL Methodology, the Planning Coordinator shall provide a technical justification to its Reliability Coordinator.~~if: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- The Facility has higher Facility Ratings as a result of a planned upgrade, addition, or Corrective Action Plan;
- Facility Rating differences are due to variations in ambient temperature assumptions;
- The Planning Coordinator provided a technical rationale for using a less limiting Facility Rating to each affected Transmission Planner and Reliability Coordinator; or
- The Transmission Planner provided a technical rationale for using a less limiting Facility Rating to each affected Planning Coordinator and Reliability Coordinator.

M1. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator implemented its process in accordance with Requirement R1.

R2. Each Planning Coordinator and each of its Transmission Planners shall implement a process to ensure that System steady-state voltage limits used in its Planning Assessment of the Near-Term Transmission Planning Horizon are equally limiting or more limiting than the System Voltage Limits ~~established~~used in ~~accordance with its~~ operations per the Reliability Coordinator's SOL Methodology. ~~If the Planning Coordinator uses less limiting System steady-state voltage limits than the System Voltage Limits established in accordance with its Reliability Coordinator's SOL Methodology, the Planning Coordinator shall provide a technical justification to its Reliability Coordinator.~~ *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- The Planning Coordinator may use less limiting System Voltage Limits if it provides a technical rationale for using a less limiting System Voltage Limits to each affected Transmission Planner and Reliability Coordinator.
- The Transmission Planner may use less limiting System Voltage Limits if it provides a technical rationale for using a less limiting System Voltage Limits to each affected Planning Coordinator and Reliability Coordinator.

M2. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator implemented its process in accordance with Requirement R2.

R3. Each Planning Coordinator and each of its Transmission Planners shall implement a process to ensure the stability performance criteria used in its Planning Assessment of the Near-Term Transmission Planning Horizon are equally limiting or more limiting than the stability performance criteria ~~established~~used in ~~its~~ operations per the Reliability Coordinator's SOL Methodology. ~~If the Planning Coordinator uses less limiting stability performance criteria than the stability performance criteria specified in its Reliability Coordinator's SOL Methodology, the Planning Coordinator shall provide a technical justification to its Reliability Coordinator.~~ *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- The Planning Coordinator may use less limiting stability performance criteria if it provides a technical rationale for using less limiting stability performance criteria to each affected Transmission Planner and Reliability Coordinator.
- The Transmission Planner may use less limiting stability performance criteria if it provides a technical rationale for using less limiting stability performance criteria to each affected Planning Coordinator and Reliability Coordinator.

M3. Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator implemented its process in accordance with Requirement R3.

~~**R4.** Each Planning Coordinator shall provide the Facility Ratings, System steady-state voltage limits, and stability performance criteria for use in its Planning Assessment to~~

~~its Transmission Planners and to requesting Planning Coordinator's. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*~~

~~**M4.** Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Planning Coordinator provided its information in accordance with Requirement R4.~~

~~**R5.** Each Transmission Planner shall use Facility Ratings, System steady-state voltage limits, and stability performance criteria in its Planning Assessment that are equally limiting or more limiting than the Facility Ratings, System steady-state voltage limits, and stability criteria provided by its Planning Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*~~

~~**M5.** Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation demonstrating the Transmission Planner used the information provided by its Planning Coordinator in accordance with Requirement R5.~~

~~**R6.**~~R4. ~~Each Planning Coordinator~~and each Transmission Planner shall communicate any instability, Cascading or uncontrolled separation identified in either its Planning Assessment of the Near-Term Transmission Planning Horizon or its Transfer Capability assessment (Planning Coordinator only) to each impacted Reliability Coordinator ~~and~~, Transmission Operator, Transmission Owner, and Generation Owner. This communication shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- ~~6~~4.1 The type of instability identified (e.g., voltage collapse, angular instability, transient voltage dip criteria violation);
- ~~6~~4.2 The associated stability criteria used as part of determining the instability;
- ~~6~~4.3 The associated Contingency(ies) ~~which result(s) in~~and any Facilities critical to the instability, Cascading or uncontrolled separation;
- ~~6.4~~4.4 A description of the studied System conditions when the instability, Cascading or uncontrolled separation was identified;
- 4.5 Any Remedial Action Scheme action, undervoltage load shedding (UVLS) action, underfrequency load shedding (UFLS) action, interruption of Firm Transmission Service, or Non-Consequential Load Loss required to address the instability, Cascading or uncontrolled separation; and
- 4.6~~.5~~ Any Corrective Action Plan associated with the instability, Cascading or uncontrolled separation.

~~**M6.**~~M4. 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 ~~R6~~R4.

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 Planning Coordinator and Transmission Planner shall keep evidence for Requirements R1 through ~~R6~~R4 for the most current year plus the previous three years.

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	~~The Planning Coordinator used less limiting Facility Ratings than the Facility Ratings established in accordance with its Reliability Coordinator's SOL Methodology, but did not provide its documented technical justification to its Reliability Coordinator.~~N/A	The Planning Coordinator or a Transmission Planner used less limiting Facility Ratings than the Facility Ratings established in accordance with its Reliability Coordinator's SOL Methodology, but ~~did not document the technical justification.~~failed to identify the exclusion criteria allowing the use of less limiting Facility Ratings.	The Planning Coordinator or a Transmission Planner failed to implement a process to ensure that Facility Ratings used in Planning Assessment are equally limiting or more limiting than those established in its Reliability Coordinator's SOL Methodology.
R2.	N/A	~~The Planning Coordinator used less limiting System steady-state voltage limits than the System Voltage Limits established in accordance with its Reliability Coordinator's SOL Methodology, but did not provide its documented technical justification to its Reliability Coordinator.~~N/A	The Planning Coordinator or a Transmission Planner used less limiting System steady-state voltage limits than the System Voltage Limits established in accordance with its Reliability Coordinator's SOL Methodology, but did not ~~document the~~provide its	The Planning Coordinator or a Transmission Planner failed to implement a process to ensure that System steady-state voltage limits used in Planning Assessments are equally limiting or more limiting than the System Voltage Limits established in accordance with its

			technical ~~justification~~rationale.	Reliability Coordinator's SOL Methodology.
R3.	N/A	~~The Planning Coordinator used less limiting stability performance criteria than the stability performance criteria established in its Reliability Coordinator's SOL Methodology, but did not provide its documented technical justification to its Reliability Coordinator.~~N/A	The Planning Coordinator or a Transmission Planner used less limiting stability performance criteria than the stability performance criteria established in its Reliability Coordinator's SOL Methodology, but did not ~~document the~~provide its technical ~~justification~~rationale.	The Planning Coordinator or a Transmission Planner failed to implement a process to ensure that stability performance criteria used in ~~planning assessments~~Planning Assessments are equally limiting or more limiting than ~~those used in operations~~the stability performance criteria established in the Reliability Coordinator's SOL Methodology.
~~**R4.**~~	~~N/A~~	~~N/A~~	~~The Planning Coordinator failed to provide the Facility Ratings, System steady-state voltage limits, and stability performance criteria to all of its Transmission Planners.~~ ~~OR~~ ~~The Planning Coordinator failed to provide one element of the required information.~~	~~The Planning Coordinator failed to provide the Facility Ratings, System steady-state voltage limits, and stability performance criteria to all of its Transmission Planners.~~ ~~OR~~ ~~The Planning Coordinator failed to provide two or more elements of the required information.~~

~~R5.~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Transmission Planner failed to use Facility Ratings, System steady-stability voltage limits, and stability performance criteria that were equally or more limiting than those provided by its Planning Coordinator.~~
~~R6~~R4.	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator ~~and~~, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain one of the elements listed in Requirement ~~R6~~R4, Parts ~~6~~4.1 – 4.6.~~5.~~	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator ~~and~~, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain two of the elements listed in Requirement ~~R6~~R4, Parts ~~6~~4.1 – 4.6.~~5.~~	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator ~~and~~, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain three elements listed in Requirement ~~R6~~R4, Parts ~~6~~4.1 – 4.6.~~5.~~	The Planning Coordinator or Transmission Planner communicated the identified instability, Cascading, or uncontrolled separation to each impacted Reliability Coordinator ~~and~~, Transmission Operator, Transmission Owner and Generator Owner, but the communication did not contain four or more of the elements listed in Requirement ~~R6~~R4, Parts ~~6~~4.1 – 4.6.~~5~~. OR The Planning Coordinator failed to communicate any identified instability, Cascading, or uncontrolled separation to each impacted

				Reliability Coordinator ~~and~~, Transmission Operator, Transmission Owner and Generator Owner.

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

Implementation Plan

Version History

Version	Date	Action	Change Tracking
1		Project 2015-09 SOL – Adopt new standard.	New

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Glossary Definition: System Operating Limit

Term: "System Operating Limit"

Definition:

Redline

All Facility Ratings, System Voltage Limits, and stability limits, applicable to ~~The value (such as MW, Mvar, amperes, frequency or volts) that satisfies the most limiting of the prescribed operating criteria for a~~ specified system configurations, used in Bulk Electric System operations for monitoring and assessing pre- and post-Contingency operating states. ~~to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to:~~

~~• Facility Ratings (applicable pre- and post-Contingency Equipment Ratings or Facility Ratings)~~
~~• transient stability ratings (applicable pre- and post- Contingency stability limits)~~
~~• voltage stability ratings (applicable pre- and post-Contingency voltage stability)~~
~~• system voltage limits (applicable pre- and post-Contingency voltage limits)~~

Clean

All Facility Ratings, System Voltage Limits, and stability limits, applicable to specified System configurations, used in Bulk Electric System operations for monitoring and assessing pre- and post-Contingency operating states.

Introduction

The standard drafting team ("SDT") for *Project 2015-09 Establish and Communicate System Operating Limits* developed these rationales to explain the modifications to the definition of the term "System Operating Limit" ("SOL ") to be incorporated into the Glossary of Terms Used in NERC Reliability Standards ("NERC Glossary"). As discussed below, the purpose of the proposed modified term is to provide greater clarity and consistency with the SOL concept and how SOLs work alongside operational performance criteria to result in reliable operations.

Background

The use of SOLs is a foundational concept in NERC's Reliability Standards, as operating within SOLs for the pre- and post-Contingency state is a primary aspect of reliable Bulk Electric System ("BES") operations. An SOL is currently defined in the NERC Glossary as:

> *The value (such as MW, Mvar, amperes, frequency or volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to:*
>
> - *Facility Ratings (applicable pre- and post-Contingency Equipment Ratings or Facility Ratings)*
> - *transient stability ratings (applicable pre- and post- Contingency stability limits)*
> - *voltage stability ratings (applicable pre- and post-Contingency voltage stability)*
> - *system voltage limits (applicable pre- and post-Contingency voltage limits)*

SOLs are the primary focus of FAC standards FAC-010, FAC-011, and FAC-014. Per these FAC standards:

- Planning Coordinators are required to have a methodology for establishing SOLs in its area for use in the planning horizon (FAC-010-3)
- Planning Coordinators and Transmission Planners are required to establish SOLs for use in the planning horizon consistent with the Planning Coordinator's SOL Methodology (FAC-014-2)
- Reliability Coordinators are required to have a methodology for establishing SOLs in its area for use in the operations horizon (FAC-011-3)
- TOPs are required to establish SOLs for use in the operations horizon consistent with the Reliability Coordinator's SOL Methodology (FAC-014-2)

FAC-011-3 requirement R2 states that the *"RC's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following."* The subsequent subparts to FAC-011-3 requirement R2 further describe pre-Contingency performance criteria (in R2.1), the post-Contingency performance criteria (in R2.2), and describe other rules related to the establishment of SOLs in the remaining subparts. The language in requirement R2 indicates that the SOLs established in accordance with requirement R2 are expected to "provide" a level of pre- and post-Contingency reliability described in the subparts of requirement R2. Accordingly, the assessments of the pre-Contingency state and the post-Contingency state are expected to be performed as part of the SOL establishment process, yielding a set of SOLs that "provide" for meeting the performance criteria denoted in FAC-011 R2 and subparts.

Requirements in FAC-014-2 then require the communication of those SOLs to the various operations and planning entities. TOP standards in effect at the time required TOPs to operate within these SOLs.
These FAC standards and related TOP standards established a construct for reliable operations. This SOL construct depicted in the body of Reliability Standards in effect in the 2007 timeframe is characterized by the following:

1. The TOPs and RCs would run studies for expected system conditions where the studies would examine the pre-Contingency state and the post-Contingency state.
2. If any performance criteria (in FAC-011 R2 subparts) were not being met in those studies, the TOP would establish an SOL which, if operated within, would result in all of those performance criteria being met.
3. The TOP would communicate those SOLs to System Operators.
4. The TOP System Operators would operate within those SOLs.

The TOP and IRO standards in effect prior to April 1, 2017 required TOPs to operate within these SOLs, the presumption being that if those SOLs were operated within in Real-time operations, then the acceptable pre- and post-Contingency operations criteria depicted in FAC-011-3 requirement R2 and subparts would be met.

It is important to note that prior to April 1, 2017 there were no Reliability Standards that required operational entities to perform assessments of the post-Contingency state in same-day or Real-time operations. Prior to April 1, 2017, the requirements associated with assessments of the post-Contingency state were folded into SOL establishment process – the establishment of SOLs that "provide" for meeting the documented pre- and post-Contingency performance criteria in FAC-011-3 requirement R2 and subparts.

The definition of SOL and the Reliability Standards that address SOLs – FAC-010, FAC-011, and FAC-014 – have remained essentially unchanged since their initial versions were approved and adopted in 2007. Since that time, many improvements have been made to the body of reliability standards, specifically those in the TPL, TOP, and IRO family of standards. The former TPL-001, -002, -003, and -004 Reliability Standards have been replaced with TPL-001-4, all of the TOP standards were replaced with the currently effective TOP-001, TOP-002, and TOP-003, and several IRO standards have been replaced as well. The definition of SOL and the FAC standards that address SOLs are inextricably linked to many of the TPL, TOP, and IRO standards, as they all address in some manner the foundational reliability concept of acceptable system performance. One of the primary objectives of Project 2015-09 is to make changes to the SOL definition and the related FAC standards to create better alignment with the currently effective TPL, TOP, and IRO standards. The SDT's proposal to revise the definition of SOL improves clarity, reduces redundancy, and creates better alignment and continuity with the currently effective TOP and IRO standards.

Due to changes in the TOP and IRO Reliability Standards that became effective on April 1, 2017, this SOL construct described by the currently effective definition of SOL and the manner in which it is used in the FAC standards is not reflective of the construct encapsulated in the operational requirements in place

today. The new TOP and IRO standards represent a new construct for managing reliability for the pre- and post-Contingency state. Under this new construct approved in Order No. 817[1]:

1. TOPs and RCs are required to ensure that an Operational Planning Analysis (OPA) is performed to assess whether the planned operations for the next-day will exceed any of its SOLs and IROLs[2]. The pre- and post-Contingency states are analyzed as part of the OPA.[3]
2. If the OPA identifies any potential exceedances, the RC and TOP must have an Operating Plan to address the exceedance.[4]
3. In Real-time, RCs and TOPs must perform Real-time Assessments (RTAs) at least once every 30 minutes to determine whether there are any expected or actual exceedances of SOLs (including IROLs) based on Real-time conditions.[5] The pre- and post-Contingency states are analyzed as part of the RTA.[6]
4. If SOL exceedances are observed in TOP Real-time monitoring or RTAs, TOPs are required to implement its Operating plan to mitigate the conditions.[7]
5. If SOL or IROL exceedances are observed in RC Real-time monitoring or RTAs, RCs are required to notify TOPs of those exceedances.[8]
6. If there is an expected or actual IROL exceedance identified in RC Real-time monitoring or RTAs, the exceedance must be resolved within the IROL T_v, which can be no longer than 30 minutes.[9]

Pursuant to the construct in the currently-effective TOP/IRO Reliability Standards, TOPs and RCs must assess system conditions, identify expected or actual SOL exceedances (including for the subset of SOLs designated as IROLs) and take steps to address any such exceedances to avoid the possibility of further deterioration in system conditions. Under this new construct, the pre- and post-Contingency states are assessed on an ongoing basis as part of OPAs and RTAs. Any SOL exceedances that are observed are required to be mitigated per the respective Operating Plans. Under this new construct, it is the OPA, the RTA, and the implementation of Operating Plans that "provide" for reliable pre- and post-Contingency operations. In the former construct, operating within the TOP-provided SOL "provided" for reliable pre- and post-Contingency

[1] *Transmission Operations Reliability Standards and Interconnection Reliability Operations and Coordination Reliability Standards*, Order No. 817, 153 FERC ¶ 61,178 (2015).

[2] IRO-008-2, Requirement R1; TOP-004-2, Requirement R1.

[3] OPA – An evaluation of projected system conditions to assess anticipated (pre-Contingency) and potential (post-Contingency) conditions for next-day operations. The evaluation shall reflect applicable inputs including, but not limited to, load forecasts; generation output levels; Interchange; known Protection System and Special Protection System status or degradation; Transmission outages; generator outages; Facility Ratings; and identified phase angle and equipment limitations. (Operational Planning Analysis may be provided through internal systems or through third-party services.)

[4] IRO-008-2, Requirement R2; TOP-004-2, Requirement R2.

[5] IRO-008-2, Requirement R4; TOP-001-3, Requirement R13.

[6] RTA – An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

[7] TOP-001-3 requirement, Requirement R14

[8] IRO-008-2 requirement, Requirement R5

[9] IRO-009-2, Requirements R1-R4; TOP-001-3, Requirement R12.

operations. The proposed revised FAC standards and the proposed revised SOL definition is intended to reflect the new construct depicted in the TOP and IRO standards.

NERC SOL Whitepaper

As discussed in the whitepaper prepared by the SDT for Project 2014-03 Revisions to TOP and IRO Standards (the "Project 2014-03 Whitepaper"), which developed the currently-effective Transmission Operations ("TOP") and Interconnection Reliability Operations and Coordination ("IRO") Reliability Standards, while the term SOL is used extensively in the NERC Reliability Standards, there is significant confusion with, and many widely varied interpretations and applications of, the term SOL. While the Project 2014-03 SDT did not seek to modify the SOL definition, they drafted the Project 2014-03 Whitepaper to describe their understanding of the SOL term/concept and to "bring clarity and consistency to the notion of establishing SOLs, exceeding SOLs, and implementing Operating Plans to mitigate SOL exceedances." The Project 2014-03 Whitepaper served as the conceptual basis for the development of the currently-effective TOP/IRO Reliability Standards.

As described in the Project 2014-03 Whitepaper, the central principles of the SOL concept in NERC's Reliability Standards is to:

1. Know the Facility Ratings, voltage limits, transient Stability limits, and voltage Stability limits, and
2. Ensure that they are all observed in both the pre- and post-Contingency state by performing a Real-time Assessment.

These principles are reflective of the new construct for managing reliability for the pre- and post-Contingency state depicted in the TOP and IRO standards created as part of Project 2014-03.

Following the development of the currently-effective TOP/IRO Reliability Standards, NERC initiated a periodic review of the requirements in the Facilities Design, Connections, and Maintenance ("FAC") group of Reliability Standards addressing SOLs. The periodic review team identified a need to revise or develop new definitions to be incorporated into the NERC Glossary to provide greater clarity and consistency in establishing SOLs and promote a common understanding of what it means to exceed SOLs. The periodic review team recognized that while the project 2014-03 Whitepaper provided clarity on the SOL concept, reliability would be further enhanced by (1) revising the SOL definition in the NERC Glossary, and (2) developing a new defined term SOL Exceedance. The periodic review envisioned that these two enhancements help to better align the definitions in the NERC Glossary with the Project 2014-03 Whitepaper and better support the SOL exceedance concept used in the TOP/IRO Reliability Standards. Subsequently, to address the issues identified in the periodic review, NERC initiated Project 2015-09 to revise the requirements for, and definitions related to, the methodology used for establishing and communicating SOLs.

In September of 2017 the standard drafting team posted a proposed definition of SOL Exceedance for informal comment. The industry responses to the draft SOL Exceedance definition indicated numerous significant concerns. Given these responses, the SDT concluded that creating a definition of SOL Exceedance that adequately reflected reliable operating principles could create too much of an unnecessary compliance burden without significant modification to the existing TOP and IRO standards. Therefore, the SDT

abandoned the idea of creating a definition for SOL Exceedance in favor of addressing the performance criteria through requirements in FAC-011-4 and FAC-014-3 similar to the way it is done in the currently effective FAC standards.

Modifications to SOL Definition

The Project 2015-09 SDT proposes to define the term System Operating Limit (SOL) as:

> *All Facility Ratings, System Voltage Limits, and stability limits, applicable to specified System configurations, used in Bulk Electric System operations for monitoring and assessing pre- and post-Contingency operating states.*

The SDT's intent was to simplify and clarify the SOL definition by eliminating ambiguities such that SOLs are easily identifiable and easily measurable. The currently-effective SOL definition states that SOLs "are based upon certain operating criteria." The modified definition eliminates the phrase "are based upon" to more accurately state that the SOLs "are" the actual operating parameters which are to be observed for the pre- and post-Contingency states, leaving no confusion as whether a Facility Rating, stability limit, or voltage limit is an SOL. The unambiguous language in the modified definition should help facilitate a more consistent application of the SOL concept within the electric industry.

Facility Ratings, System Voltage Limits, and stability limits are the three types of operating criteria included in the existing SOL definition and carried forward into the modified definition that must be accounted for to ensure reliable operations. Facility Ratings must be established in accordance with Reliability Standard FAC-008-3. System Voltage Limits, as discussed below, is proposed to be defined as "the maximum and minimum steady-state voltage limits (both normal and emergency) that provide for acceptable System performance." Stability limits includes both transient stability limits and voltage stability limits. The intent of using the "stability limit" term (as opposed to the NERC Glossary term "Stability Limit") is to allow for a number of different types of stability-related limitations or phenomena, including, but not limited to, sub-synchronous resonance (SSR), phase angle limitations, transient voltage limitations on equipment, and weighted short-circuit ratio (WSCR). The Glossary term "Stability Limits" is not appropriate for use in the revised definition because its use is limited to a maximum power flow value. While some entities may use maximum power flow values as a means by which to prevent instability, this approach represents only one particular method and may be too restrictive for some entities. Reliability tools allow entities to monitor and control parameters other than maximum power flow values in order to demonstrate acceptable stability performance.

Unlike the existing SOL definition, the proposed definition includes the phrase "used in Bulk Electric System operations" to distinguish those Facility Ratings, voltage limits, and stability limits that are used in planning. The SDT determined that the SOL concept should be limited to the operational time horizon and thus proposes to retire FAC-010-3. The Facility Ratings, voltage limits, and stability criteria used in the planning horizon are developed according to FAC-008-3 and TPL-001-4 and, as a result, there was no additional reliability need to require Planning Authorities to develop SOLs to be used in the planning horizon. The SDT concluded, however, that there was a reliability need to coordinate the Facility Ratings, voltage limits, and

stability criteria used in planning with those used in operations. The SDT developed proposed Reliability Standard FAC-015-1 to address that issue.

As discussed in detail below, the SDT determined that references to "most limiting criteria" and "acceptable reliability criteria", and the manner in which the "specified system configuration" and the "pre- and post-contingency" phrases were used in the currently-effective definition of SOL were adding to industry confusion as to what constitutes an SOL.

Most limiting Criteria – The SDT concluded that removing the "most limiting criteria" concept in favor of designating all Facility Ratings, System Voltage Limits, and stability limits as SOLs is better aligned with the requirements in the TOP/IRO Reliability Standards. As noted above, under the TOP/IRO Reliability Standards, each RC and TOP must perform Operational Planning Analysis (OPAs) and Real-time Assessments (RTAs) to assess conditions in the day ahead and Real-time horizon and, if it identifies any actual, expected or potential SOL exceedance, take appropriate mitigating action to maintain pre- and post-Contingency reliable operations. Under the currently-effective SOL definition, RCs and TOPs must initially determine which operating parameter is the most limiting at that point in time to be designated as the SOL and then determine if there are any actual, potential, or expected exceedances of that SOL. The SDT understands that this has caused some confusion within industry. Specifically, it may be unclear in Real-time operations when an SOL ceases to be an SOL because it is no longer the "most limiting criteria." Confusion is introduced when the most limiting criteria (and thus the SOL) changes from one RTA to the next.

The SDT determined that it is more straightforward to simply categorize all Facility Ratings, System Voltage Limits, and stability limits as SOLs. In performing OPAs and RTAs, RCs and TOPs should be assessing conditions as it relates to any operating parameter or reliability limit, not the most limiting parameter or limit based on a particular prior analysis. Under the new TOP and IRO requirements, RCs and TOPs are assessing conditions on an ongoing basis through OPAs and RTAs to determine whether there are any actual, potential, or expected exceedances of any Facility Rating, System Voltage Limit, or stability limit, which would necessarily include the most limiting of those parameters/limits. In this manner, the "most limiting criteria" concept is subsumed within the requirements of the TOP/IRO Reliability Standards and it is not necessary that it be included in the SOL definition. In short, the proposed SOL definition creates a simplified approach. There is no need to continuously identify and communicate the ever-changing "most limiting" criteria. Entities must simply operate – and plan to operate – to prevent any exceedance of all Facility Ratings, System Voltage Limits, and stability limits.

The SDT determined that the removal of the "most limiting criteria" from the SOL definition represents an improvement to reliability. The "most limiting criteria" can adversely impact reliability by masking instability risks that may exist slightly beyond the point of the most limiting condition. To illustrate, where prior studies indicate that a thermal limitation is the "most limiting criteria," if the studying entity does not study the performance of the system appreciably beyond this thermal limitation to reasonably expected stressed conditions, it cannot be safely concluded that a more significant instability risk does not exist slightly beyond the point where the "most limiting criteria" exists. Because actions may be taken in the actual system conditions that mitigate thermal and voltage limitations identified as a "most limiting criteria", it may be necessary to identify where subsequent operation may approach a point of instability. Consistent with this

concept, the RC and its TOPs have the responsibility of establishing stability limits in accordance with the Reliability Coordinator's SOL Methodology, as required by FAC-011-4 Requirement R4 and FAC-014-3 Requirements R2 and R4.

Acceptable Reliability Criteria – The SDT determined that the "acceptable reliability criteria" concept is best addressed through requirement language and that the SOL definition should focus simply on what constitutes an SOL. Taken together, the operations performance criteria in FAC-011-4 requirement R6 and the corresponding requirement R7 in FAC-014-3 adequately addresses operation within acceptable reliability criteria.

Specified System Configuration – The SDT proposes to retain the reference to "specified system configuration" due to the fact that stability limits in particular are typically dependent on system configuration. While Facility Ratings and System Voltage Limits are not typically dependent upon system configuration, there may be times where they may be dependent on System configuration. For example, if a transmission line is connected by two circuit breakers at one end of the line, and one of those two circuit breakers is open, the value of the Facility Rating for line could be reduced due to current carrying capability of the remaining in-service circuit breaker.

Pre- and Post-Contingency – The currently effective SOL definition specifies that each of the listed operating limit types are applicable for both the pre- and post-Contingency states. The SDT determined that the pre- and post-Contingency concept needed to be retained; however, it should be used in a manner consistent with the construct depicted in the new TOP and IRO standards rather than the old construct where the SOL itself "provided" for pre- and post-Contingency acceptable performance. The proposed definition makes it clear that both the pre-Contingency state and the post-Contingency state must be considered when evaluating the System performance for Facility Ratings, System Voltage Limits, and stability limits. As OPAs and RTAs are the mechanisms in the Reliability Standards for determining potential SOL exceedances (OPA) and actual SOL exceedances (RTA),[10] the definition of SOL should support the concept that both the pre- and post-Contingency states should be accounted for.

One aspect of the improved clarity of the revised definition of SOL is seen in its intended use. Under the revised definition, SOLs are intended to be used as an input into the OPA and RTA process.[11] The OPA and RTA process itself examines SOLs for the pre- and post-Contingency states and determines whether the SOLs are being exceeded. Accordingly, while SOLs are an input to the OPA and RTA process, SOL exceedance is the output of the OPA and RTA process. FAC-014-3 requirement R7 effectively stipulates that the operations performance criteria denoted in FAC-011-4 requirement R6 must be used in OPAs, RTAs, and Real-time monitoring when identifying SOL exceedances.

[10] In Order No. 705 (at P 162), the Commission stated that system performance is determined through studies, stating "the Commission believes that to demonstrate the pre- and post-contingency performance metrics required by [FAC-010-1] Requirements R2.1-R2.2 an assessment or analysis would need to be performed. As such, Requirements R2.1-R2.2 provide for actions that go beyond NERC's characterization of the subject of the requirements as limited to a list of topics that must be included in a methodology. Therefore, we conclude that these Requirements are more Docket No. RM07-3-000 - 79 - properly treated as implementation or operational requirements that may have a direct impact on reliability."

[11] Some Reliability Coordinators and Transmission Operators may establish stability limits in the context of an OPA or RTA. For entities who adopt this approach, the stability SOL would be established – and its exceedance determined – as part of the OPA or RTA.

Lastly, as with the currently-effective SOL definition, the proposed SOL definition does not include reference to IROLs. IROLs, as currently defined, are a subset of SOLs that, if exceeded, "could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the BES." The determination of when an SOL should be designated as an IROL is most appropriately addressed in the RC's SOL methodology. There is no need to mention IROLs in the definition of SOL.

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 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	March 14, 2017 – April 11, 2017
45-day formal comment period with initial ballot	September 14 – October 30, 2017
45-day formal comment period with additional ballot	March 16 – April 30, 2018
45-day formal comment period with additional ballot	June 3 – July 18, 2019
45-day formal comment period with additional ballot	November 1 – December 16, 2019
10-day final ballot	~~January 24 –~~ February ~~3,~~ 2020

Anticipated Actions	Date
NERC Board	May 2020

A. Introduction

1. **Title:** Cyber Security – BES Cyber System Categorization

2. **Number:** **CIP-002-6~~5.1a~~**

3. **Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems 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 ~~Special Protection System or~~ Remedial Action Scheme where the ~~Special Protection System or~~ 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. 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 where the ~~Special Protection System or~~ 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.

4.2.3.1. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.2. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.3. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

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.

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

5. Effective Date: See Implementation Plan for CIP-002-6.

~~**1. 24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~**2.** In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

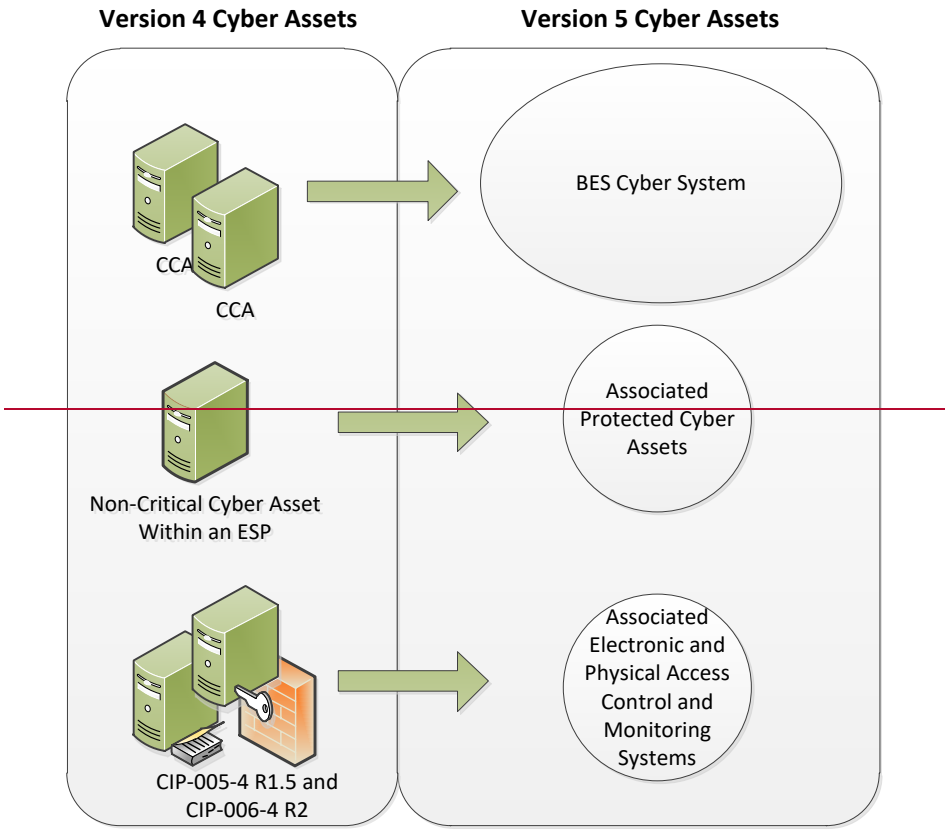
6. Background: This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the 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

~~One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.~~



~~In t~~Transitioning ~~from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4).~~ 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 ~~Version 5~~ 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, ~~Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11~~ Section 1 or Section 2, and listed in Section 3 default to ~~be~~ 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 ~~Version 5~~ 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 ~~may~~ include, to the extent they are within the ESP: file servers, ~~ftp~~ 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.** ~~Special Protection Systems~~ Remedial Action Schemes 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~~s~~ according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber System~~s~~ 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).

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.

R2. ~~The~~ 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.

~~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 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 ~~Assessment~~ Enforcement Program ~~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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Systems, five percent or fewer of identified BES Cyber Systems 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 Systems, five or fewer identified BES Cyber Systems 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 Systems, five percent or fewer high or medium BES Cyber	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems 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 Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR	Systems, more than 15 percent of identified BES Cyber Systems 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 Systems, more than 15 identified BES Cyber Systems 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 Systems, more than 15 percent of high or medium impact BES

	Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.
R2.	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of

	OR The Responsible Entity did not complete its approval of the identifications required by 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. (R2.2)	The Responsible Entity failed to complete its approval of the identifications required by 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. (R2.2)	The Responsible Entity failed to complete its approval of the identifications required by 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. (R2.2)	the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Associated Documents

- See Implementation Plan for CIP-002-6.
- 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.
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	TBD	Criteria for 2.12 was modified	

~~CIP-002-5.1a - Attachment 1~~

~~Impact Rating Criteria~~

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 ~~(H)~~

Each BES Cyber System 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 ~~(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.

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 that meet this criterion are those shared 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.

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 ~~Special Protection System (SPS),~~ Remedial Action Scheme (RAS)~~,~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed 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 (H) 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 used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.~~ 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 ~~(H)~~ 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 ~~(L)~~

BES Cyber Systems 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. ~~Special Protection Systems~~ Remedial Action Schemes 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-~~5.1a~~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-~~5.1a~~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-~~5.1a~~6
CIP-002-~~5.1a~~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-~~5.1a~~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	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that 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)
- ~~Special Protection Systems or~~ 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.
~~Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.~~

Attachment 1
Overall Application
In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System 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-002-5.1a, 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 ~~(H)~~

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, BA~~a~~s, 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 BA~~a~~s with significant impact are covered under this criterion.

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

Medium Impact Rating (M)

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 ~~Special Protection Systems and~~ Remedial Action Schemes as medium impact. ~~Special Protection Systems and~~ Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and 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 (IROLs). 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 ~~document~~ "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", document, ~~Attachment 1,~~ the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

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 ~~Special Protection Systems (SPS),~~ Remedial Action Schemes (RAS)~~,~~ or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- 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 ~~as~~ medium impact ~~those~~ BES Cyber Systems ~~used by and at~~ associated with Control Centers and backup Control Centers, including associated data centers ~~performing the functional obligations of a~~, that monitor and control BES Transmission ~~Operator~~ lines with an aggregated weighted value of 6000 or higher, and that have not already been ~~categorized as high impact~~ 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

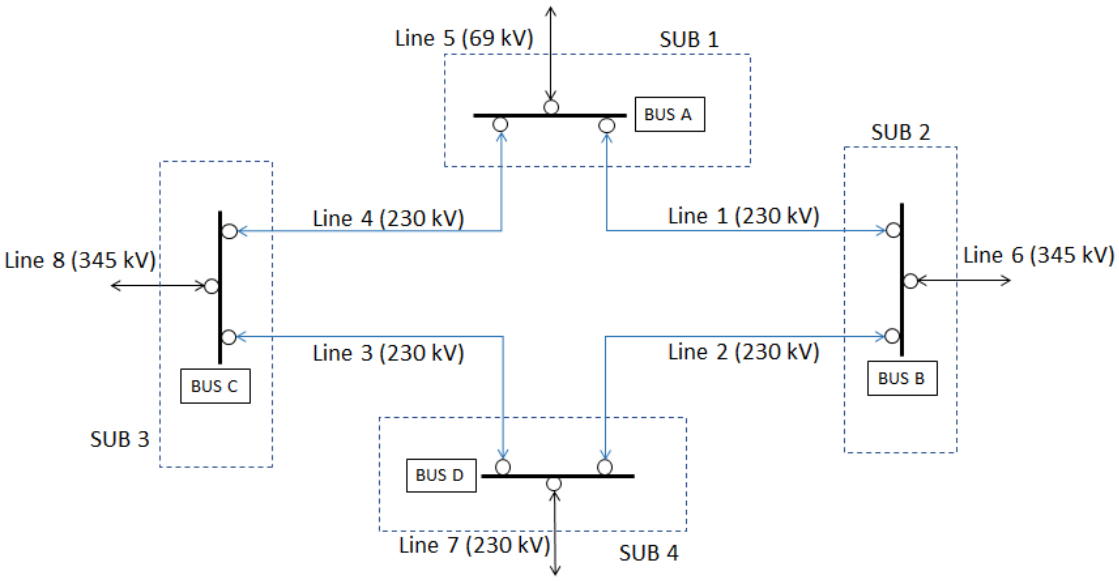
Control Centers validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.

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

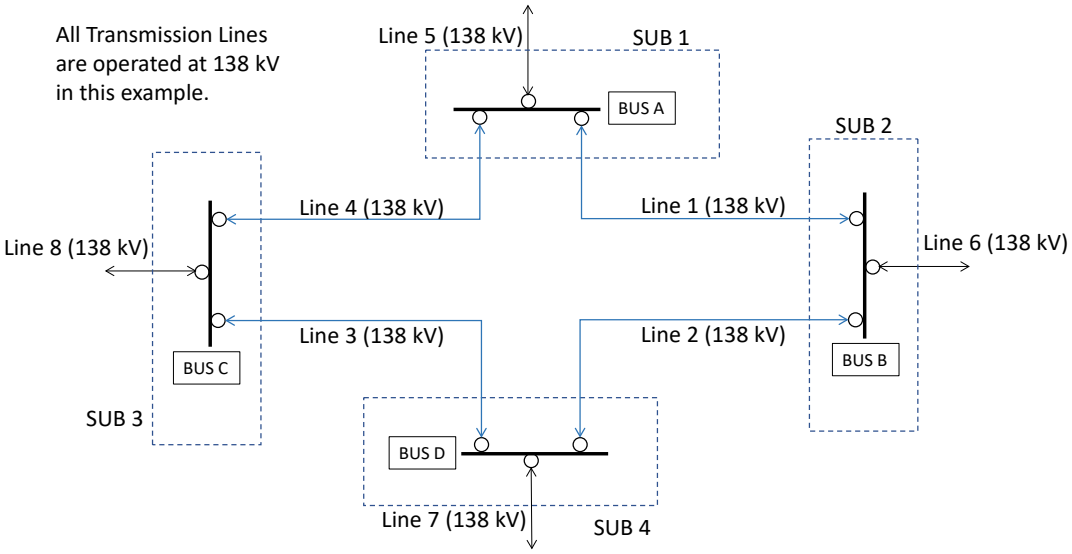
The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in 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 ~~high impact.~~ 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 ~~(L)~~

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. ~~BES Cyber Systems not categorized in high impact or medium impact 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.

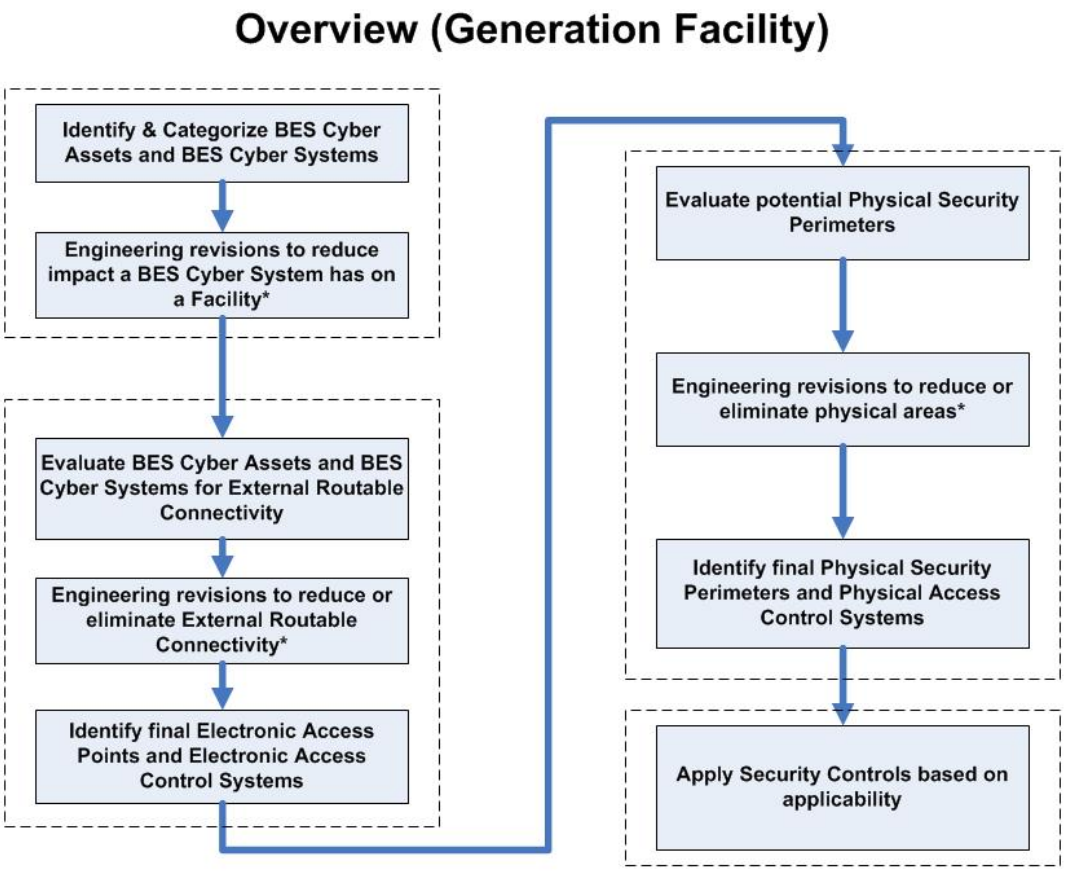
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific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



* - 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.

Appendix 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:

a. 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

Completed Actions	Date
Standards Committee 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
Informal comment period	March 14, 2017 – April 11, 2017
45-day formal comment period with initial ballot	September 14 – October 30, 2017
45-day formal comment period with additional ballot	March 16 – April 30, 2018
45-day formal comment period with additional ballot	June 3 – July 18, 2019
45-day formal comment period with additional ballot	November 1 – December 16, 2019
10-day final ballot	February 2020

Anticipated Actions	Date
NERC Board	May 2020

A. Introduction

1. **Title:** Cyber Security – BES Cyber System Categorization

2. **Number:** **CIP-002-6**

3. **Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems 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 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.

4.2.3.1. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.2. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.3. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

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.

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

5. Effective Date: See 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 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 according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber System 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).

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.

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 #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Systems, five percent or fewer of identified BES Cyber Systems 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 Systems, five or fewer identified BES Cyber Systems 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 Systems, five percent or fewer high or medium BES Cyber	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems 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 Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR	Systems, more than 15 percent of identified BES Cyber Systems 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 Systems, more than 15 identified BES Cyber Systems 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 Systems, more than 15 percent of high or medium impact BES Cyber

	Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.
R2.	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of

	OR The Responsible Entity did not complete its approval of the identifications required by 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. (R2.2)	The Responsible Entity failed to complete its approval of the identifications required by 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. (R2.2)	The Responsible Entity failed to complete its approval of the identifications required by 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. (R2.2)	the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Associated Documents

- See Implementation Plan for CIP-002-6.
- 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.
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	TBD	Criteria for 2.12 was modified	

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 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, 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.

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 that meet this criterion are those shared 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.

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 (H) 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 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 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	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements

or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that 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-002-5.1a, 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 (M)

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 (IROLs). 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 aggregated 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.

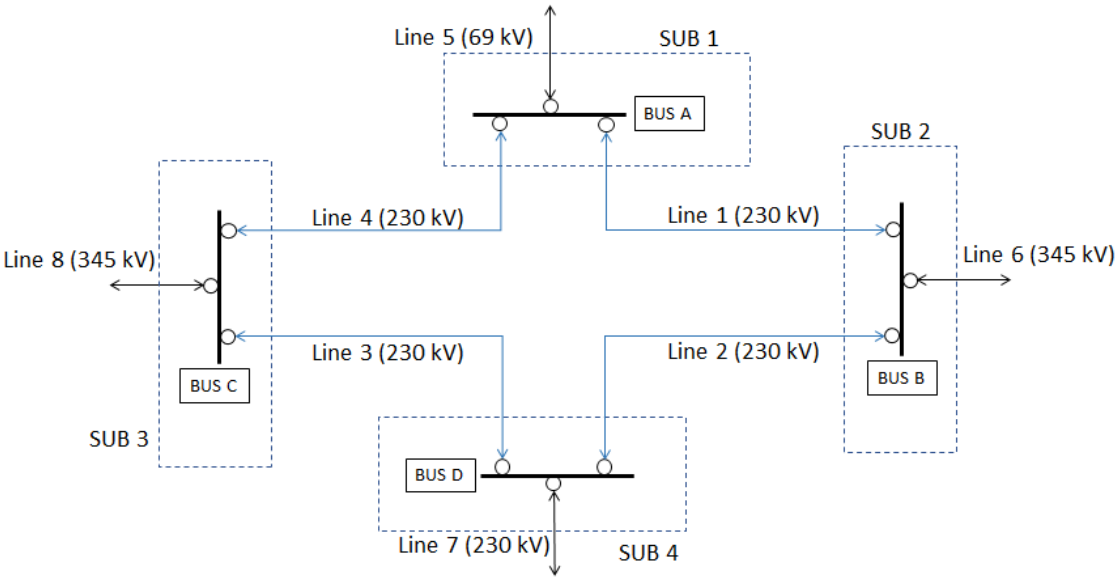
  The total aggregated weighted value is used to account for the impact to the BES. The 6000 aggregate weighted value threshold defined in criterion 2.12 provides a sufficient differentiation for medium and low impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission 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

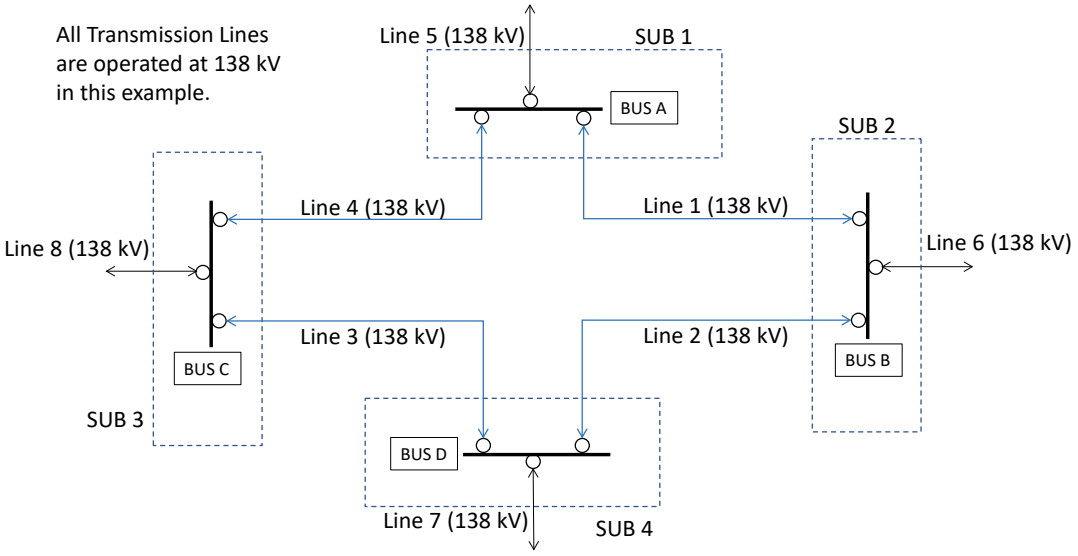
The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in 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.

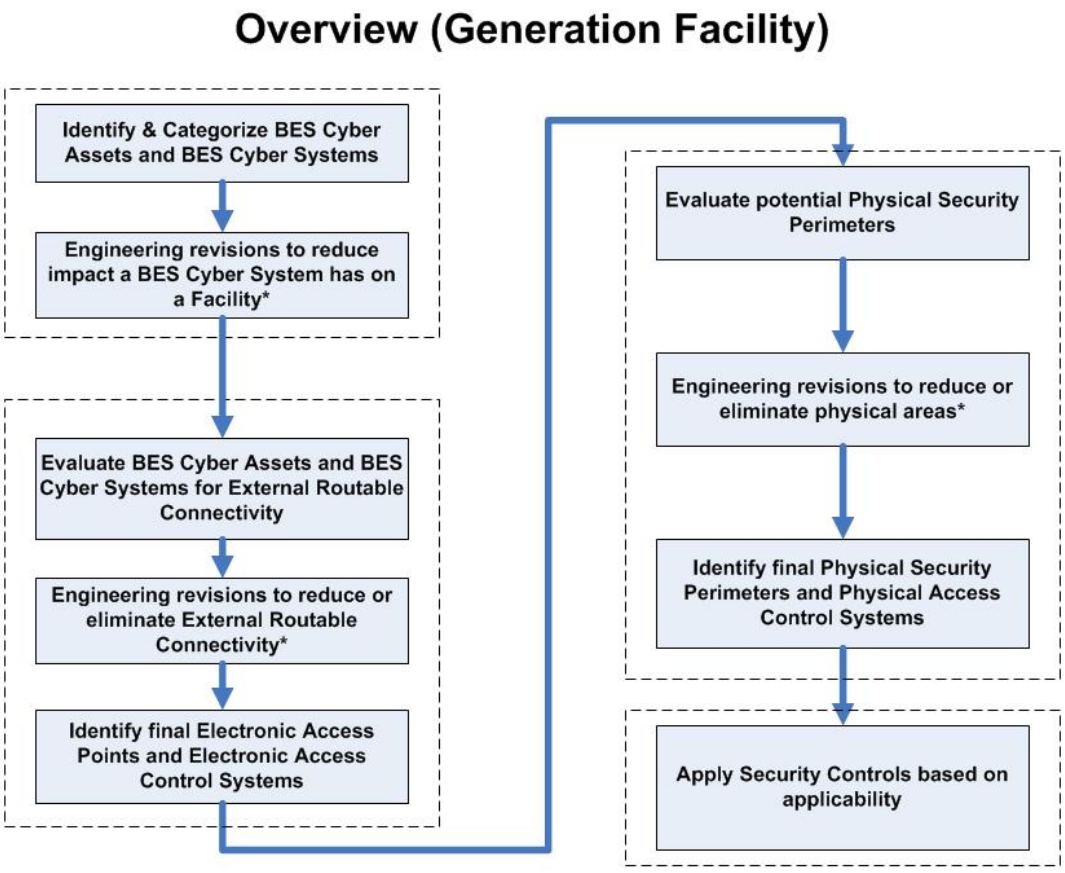
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific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



* - 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.

Appendix 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:

a. 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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-002-6

Applicable Standard(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization

Requested Retirement(s)

- Reliability Standard CIP-002-5.1a – Cyber Security – BES Cyber System Categorization

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

This Implementation Plan includes ~~a~~ phased-in implementation dates for Criterion 2.12 of CIP-002-6, Attachment 1. The phased-in implementation dates allow Responsible Entities[1] a longer implementation period if the revisions to the Criterion would result in a higher impact level categorization of a BES Cyber System.

Effective Date and Phased-In Implementation Dates

The effective date for proposed Reliability Standard CIP-002-6 is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion of it),

[1] As used in the CIP Reliability Standards, a Responsible Entity refers to a registered entity responsible for the implementation of and compliance with a particular requirement.

the additional time for compliance with that section is specified below. The phased-in implementation date for those particular sections is the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter immediately after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter immediately after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements
Responsible Entities shall initially comply with the periodic requirements in CIP-002-6, Requirement R2 within 15 calendar months of their last performance of Requirement R2 under CIP-002-5.1a.

Phased-in Implementation Date for CIP-002-6, Requirement R1, Attachment 1 Criterion 2.12
If the revisions to Criterion 2.12 of Attachment 1 to CIP-002-6 result in a higher impact level categorization of a BES Cyber System, the Responsible Entity shall not be required to identify that BES Cyber System as that higher categorization nor apply the requirements throughout the CIP standards applicable to that higher categorization until 24 months after the effective date of CIP-002-6. Until that time, the Responsible Entity shall continue to identify that BES Cyber System consistent with its existing categorization under CIP-002-5.1a, Requirement R1, Part 1.3.

Planned or Unplanned Changes
The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5 shall apply to CIP-002-6. The Implementation Plan associated with CIP-002-5 provided as follows with respect to planned and unplanned changes (with conforming changes to the version numbers of the standard):

Planned Changes
Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Rresponsible Eentity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For *planned* changes resulting in a higher categorization, the ~~r~~Responsible ~~e~~Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* ~~above~~of the CIP-002-5.1a Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the ~~r~~Responsible ~~e~~Entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the ~~r~~Responsible ~~e~~Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* ~~above~~of the CIP-002-5.1a Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to M~~m~~Medium - i~~I~~mpact BES Cyber Systems

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Newly categorized medium impact BES Cyber System	12 months
Responsible ~~e~~Entity identifies its first high impact or medium impact BES Cyber System (i.e., the ~~r~~Responsible ~~e~~Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Reliability Standard CIP-002-5.1a

Reliability Standard CIP-002-5.1a shall be retired immediately prior to the effective date of Reliability Standard CIP-002-6 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-002-6

Applicable Standard(s)

- Reliability Standard CIP-002-6 – Cyber Security - BES Cyber System Categorization

Requested Retirement(s)

- Reliability Standard CIP-002-5.1a – Cyber Security - BES Cyber System Categorization

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

This Implementation Plan includes phased-in implementation dates for Criterion 2.12 of CIP-002-6, Attachment 1. The phased-in implementation dates allow Responsible Entities[1] a longer implementation period if the revisions to the Criterion would result in a higher impact level categorization of a BES Cyber System.

Effective Date and Phased-In Implementation Dates

The effective date for proposed Reliability Standard CIP-002-6 is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion of it),

[1] As used in the CIP Reliability Standards, a Responsible Entity refers to a registered entity responsible for the implementation of and compliance with a particular requirement.

the additional time for compliance with that section is specified below. The phased-in implementation date for those particular sections is the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

Reliability Standard CIP-002-6 - Cyber Security – BES Cyber System Categorization
Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter immediately after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter immediately after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements
Responsible Entities shall initially comply with the periodic requirements in CIP-002-6, Requirement R2 within 15 calendar months of their last performance of Requirement R2 under CIP-002-5.1a.

Phased-in Implementation Date for CIP-002-6, Requirement R1, Attachment 1 Criterion 2.12
If the revisions to Criterion 2.12 of Attachment 1 to CIP-002-6 result in a higher impact level categorization of a BES Cyber System, the Responsible Entity shall not be required to identify that BES Cyber System as that higher categorization nor apply the requirements throughout the CIP standards applicable to that higher categorization until 24 months after the effective date of CIP-002-6. Until that time, the Responsible Entity shall continue to identify that BES Cyber System consistent with its existing categorization under CIP-002-5.1a, Requirement R1, Part 1.3.

Planned or Unplanned Changes
The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5 shall apply to CIP-002-6. The Implementation Plan associated with CIP-002-5 provided as follows with respect to planned and unplanned changes (with conforming changes to the version numbers of the standard):

Planned Changes
Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For *planned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* of the CIP-002-5.1a Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* of the CIP-002-5.1a Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Reliability Standard CIP-002-5.1a

Reliability Standard CIP-002-5.1a shall be retired immediately prior to the effective date of Reliability Standard CIP-002-6 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2017-01 Modifications to BAL-003-1.1

Do not use this form for submitting comments. Use the electronic form to submit informal comments on **Project 2017-01 Modifications to BAL-003-1.1**. The electronic form must be submitted by **8 p.m. Eastern, Wednesday, April 17, 2019**.

Documents and information about this project are available on the project page. If you have questions, contact Standards Developer, Laura Anderson (via email) or at (404) 446-9671.

Background

Project 2017-01 Modifications to BAL-003-1.1

The purpose of this project is to review the issues identified in Phase II of the Standard Authorization Request (SAR) and make corresponding modifications to BAL-003-2, as necessary.

Standard affected: BAL-003-2

The informal comment period for this survey is seeking inputs into the standard drafting team's (SDT) Phase II modifications to BAL-003-2, as identified in the SAR:

- Make the Interconnection Frequency Response Obligation (IFRO) calculations and associated allocations: 1) more reflective of current conditions; 2) consider all characteristics affecting Frequency Response (e.g., load response, mix and type of generation); 3) include all applicable entities; and 4) be as equitable as possible; and
- Frequency Response Measure (FRM): 1) ensure that over-performance by one entity does not negatively impact the evaluation of performance by another; 2) measure types/periods of response in addition to secondary Frequency Response, particularly primary Frequency Response; 3) include all applicable entities; and 4) make allocations as equitable as possible.

NERC has been studying Frequency Response for several years, with the most recent study completed in 2018. The results of the studies have not identified any significant detrimental changes in Frequency Response on any Interconnection. This does not mean that potential changes in the resource mix and operation of the grid will not impact the response currently seen on the interconnections. Because of comments received, the drafting team is looking at several different areas of BAL-003 that could be changed to potentially improve the reliability and compliance process.

In this highly-complex standard, the drafting team has found that simple yes/no answers or selection of alternatives fail to communicate the concerns of the commenters effectively; this results in the drafting team having to guess the reasons for the answers provided. Consequently, the drafting team requests that all answers include an explanation of why the comment provides the best answer to the question asked. This allows the drafting team to understand the reasons for the comments supplied and enables

the team to modify the standard to balance the reliability needs of the BES with the goals of those commenting.

Comments have stated that a two-year lag between the operation numbers used for allocation and the operation of the grid is too much lag. The current process uses the load and generation numbers as reported in the FERC 714 report.

Please provide your responses to the questions listed below, along with any detailed comments.

Questions

1. What is the maximum acceptable lag in the data to be used for IFRO allocation and minimum frequency bias determination?

   a. 2 Years ☐

   b. 1 Year ☐

   c. Quarterly ☐

   d. Forward-looking forecast ☐

   Please explain your response:

2. If the SDT moves away from using FERC 714 data, should it consider:

   a. Load and generation ☐

   b. Just generation ☐

   c. Just load ☐

   Please explain your response, including the source of the data you recommend:

Comments have been received stating that the current process recognizes there may be multiple sources of response, including, but not limited to, native load, contracted loads and generation. The comments further suggest that the current process requirement on the Balancing Authority (BA) be supplemented (or replaced) with a requirement on other entities, specifically the Generator Owner.

3. FERC's Order 842 regarding new Generator Interconnection Agreements requires newly interconnecting large and small generating facilities, both synchronous and non-synchronous, to install, maintain, and operate equipment capable of providing primary Frequency Response as a condition of interconnection. Should there be a similar requirement in BAL-003 related to all equipment capable of providing primary Frequency Response?

   ☐ Yes

   ☐ No

   Please explain your response:

Comments have been received stating there is a concern that the existing median methodology could be subject to reduced performance once a sufficient level of compliance has been achieved. One means of addressing this concern is to have an operational planning process and monitoring Real-time Frequency Response capability.

4. Should there be a requirement for Real-time Frequency Responsive Reserve (FRR) (similar to BAL-002, Requirement R2)?

   ☐ Yes

   ☐ No

   ☐ Other

   Please explain your response:

5. As a BA, do you calculate and monitor online FRRs in Real-time? If no, please explain impediments to doing so, if applicable. If yes, please describe your methodology.

   ☐ Yes

   ☐ No

   ☐ N/A

   Please explain your response:

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

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 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-~~6~~7

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   ~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

   ~~**4.1.6.**~~**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-~~6~~7:

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

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

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

5. Effective Dates:

See Implementation Plan for CIP-004-~~6~~7.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or

CIP-004-~~6~~7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• 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-~~6~~7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~6~~7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.~~; and~~ ~~4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and~~,~~ unescorted physical access into a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

~~CIP-004-7 Table R4 – Access Management Program~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~4.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS; and~~ ~~3. PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~2. EACMS; and~~ ~~2. PACS~~	~~Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.~~	~~An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:~~ ~~1. A dated listing of authorizations for BES Cyber System information;~~ ~~2. Any privileges associated with the authorizations; and~~ ~~3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions~~

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

~~CIP-004-6~~7 Table R5 – Access Revocation			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~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-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~4~~3	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 Part~~s~~ 5.1~~ or 5.3~~) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~5~~4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance ~~Violation~~ Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic access~~,~~or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its 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-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its 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-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~locations, privileges were incorrect or unnecessary. (4.4)~~			
R5	**Same Day Operations and Operations Planning**	**Medium**	~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or~~,~~ unescorted physical access~~, or BES Cyber System Information storage locations~~. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~of the termination action. (5.3)~~ ~~OR~~ The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4~~3~~) 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-~~6~~7)			
			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.~~5~~4) 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-~~6~~7)			
			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.~~5~~4)			

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	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES

Version	Date	Action	Change Tracking
			Cyber System Information.

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~~

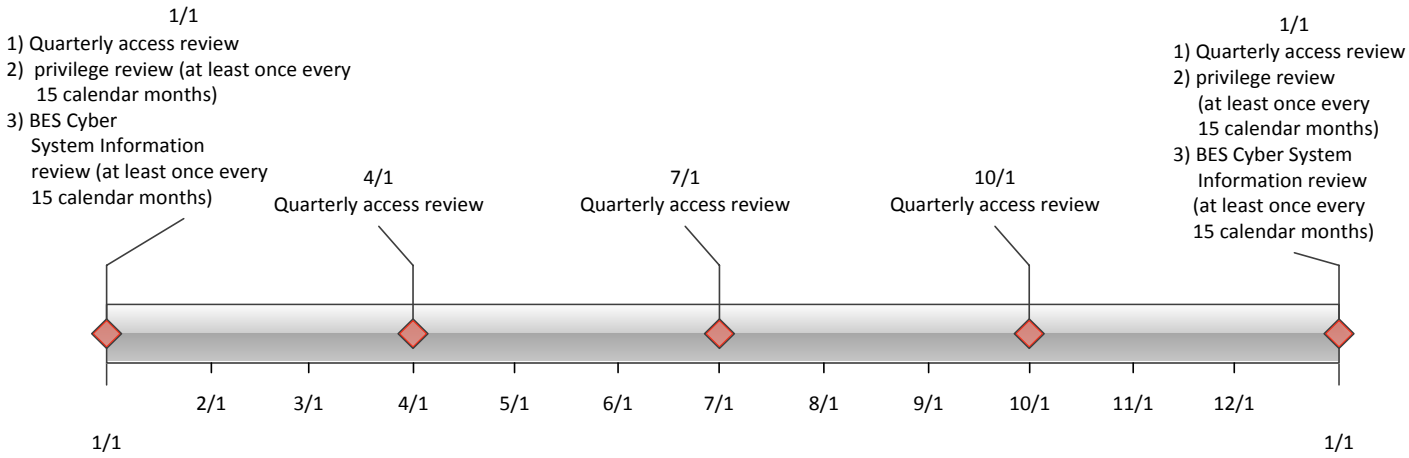
~~collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under 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 the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.~~

~~**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

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 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-004-7

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each 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 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-004-7:

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

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

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

5. Effective Dates:

See Implementation Plan for CIP-004-7.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, emails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• 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-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access into a Physical Security Perimeter.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic accessor unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	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)	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 incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3)			
R5	**Same Day Operations and Operations Planning**	**Medium**	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. (5.3) 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 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 access following reassignments 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 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 access following reassignments or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (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 removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) 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)	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)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.4)			

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	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES

Version	Date	Action	Change Tracking
			Cyber System Information.

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-7. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-004-7, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4(CIP-011-3 Requirement R1, Part 1.6) and a portion of Part 4.1(CIP-011-3 Requirement R1, Part 1.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R5

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R5

The VSL has been revised to reflect the removal of Part 5.3(CIP-011-3 Requirement R1, Part 1). The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 to CIP-011-3

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-011 Requirement R1.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R4, Part 4.1.3 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.3 Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Access to designated storage locations for BES Cyber System Information moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus changed from access to designated storage locations to access to BES Cyber System Information.
CIP-004-6, Requirement R4, Part 4.4 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.	CIP-011-3, Requirement R1, Part 1.6 Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determines are necessary for performing assigned work functions.	15-month entitlement reviews to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls. Focus of verification changed from designated storage locations to BES Cyber System Information.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R4, Part 5.3 For termination actions, revoke the individual's current 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.	CIP-011-3, Requirement R1, Part 1.5 For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Next calendar day termination actions for those with access to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus of termination actions changed from access to designated storage locations to access to BES Cyber System Information.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-004-7

December 2019

CIP-004-7 – Personnel & Training

Rationale for Requirement R4

The standard drafting team (SDT) utilized the concept of separating the association of BES Cyber System Information (BCSI) and the BES Cyber System with associated applicable systems within the CIP-004 Standard. This approach was decided to allow for maturity in the CIP-011 Information Protection Standard, facilitate future iterations of CIP-004, and remove confusion regarding protection of BCSI and BES Cyber System with associated applicable systems due to the Applicable Systems column in the requirement.

CIP-011 will include the complete lifecycle of information related to BCSI (i.e., identification, protection, access management, and disposal), thus focusing on protection and access management on BCSI itself, as appropriate. The diverse needs of entities can be addressed directly without causing confusion or affecting access management of BCSI and associated repositories. This will allow future standard development for information protection to mature in an easier fashion without disturbing requirements that involve access management of BES Cyber Systems and their associated applicable systems that may require electronic and /or physical security perimeters.

Physical access to BCSI can now be addressed separately from access to specific host media / devices whether a designated storage location or a BES Cyber System and its associated applicable systems.

This will allow the SDT the ability to move away from specifically having requirements around putting controls pertaining to designated storage locations or BES Cyber Systems and their associated applicable systems. The focus will move to implementing controls to address BCSI regardless of where the media resides at any given time.

Rationale for Requirement R4, Part 4.1.3

The intent of Requirement R4, Part 4.1.3, is now addressed in the revised version of CIP-011 regarding BCSI access management; therefore, the language was removed from Requirement R4, Part 4.1.

Rationale for Deletion of Requirement R4, Part 4.4

The intent of Requirement R4, Part 4.4, is now addressed in the revised version of CIP-011 regarding BCSI access management; therefore, this requirement is being recommended for retirement.

Rationale for Deletion of Requirement R5, Part 5.3

The intent of Requirement R5, Part 5.3, is now addressed in the revised version of CIP-011 regarding BCSI access management; therefore, this requirement is being recommended for retirement.

Rationale for Deletion of Requirement R5, Part 5.4

The language connecting this requirement to Requirement R5, Part 5.3, has been removed since the SDT is recommending the retirement of Requirement R5, Part 5.3.

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-004-6 standard to preserve any historical references.

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.

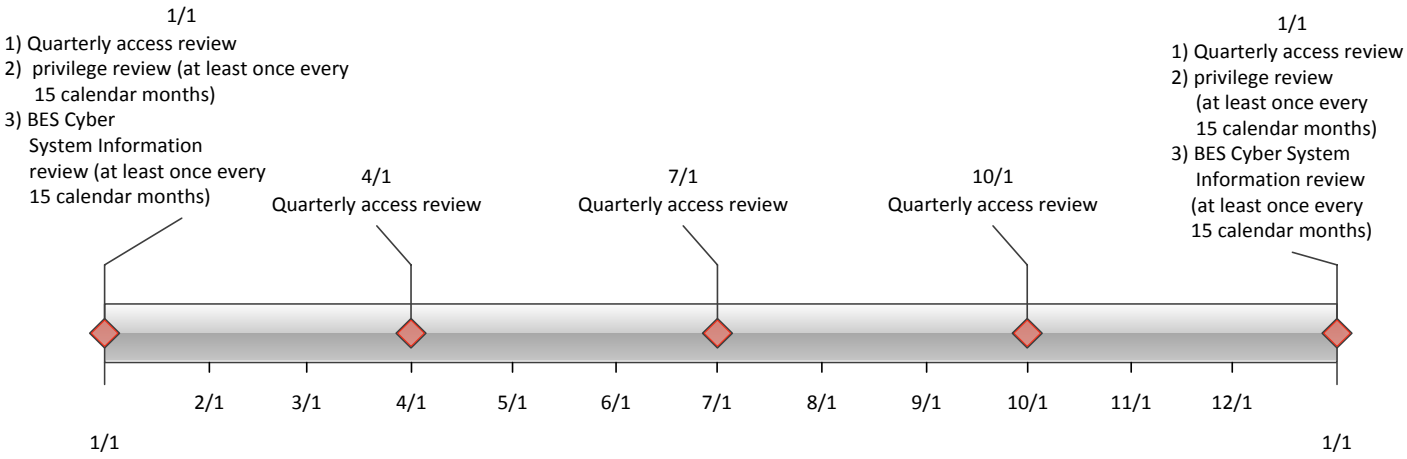
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. 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 accounts 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

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 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-~~2~~3

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS)~~ or Remedial Action Scheme (RAS) where the ~~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-~~2~~3:

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

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

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

5. Effective Dates:

See Implementation Plan for CIP-011-~~2~~3.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the 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 "Applicability 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-~~2~~3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~2~~3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.1	System information pertaining to: High ~~-~~Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA	~~Method~~Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Examples of acceptable evidence include, but are not limited to, the following: • Documented ~~method~~ process(es) to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • ~~Repository or electronic and physical~~ Storage locations identified ~~designated~~ for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.2	BES Cyber System Information as identified in Requirement R1 Part 1.1. ~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~PACS~~	~~Procedure~~Method(s) to prevent unauthorized access to ~~for protecting and securely handling~~ BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during~~, including~~ storage, transit, use, and disposal~~-~~.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to prevent the unauthorized access to ~~Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of~~ BES Cyber System Information (e.g., encryption of ~~; or~~ • ~~Records indicating that~~ BES Cyber System Information and key management program, retention in the Physical Security Perimeter)~~is handled in a manner consistent with the entity's documented procedure(s)~~.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure

1.4	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of acceptable evidence may include, but are not limited to, dated documentation of all of the following: • Methodology(ies) used to perform risk assessments • Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity; • Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and • Dated documentation of action plans and statuses of remediation and/or mitigation action items.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. [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-011-3 Table R2 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R3~~2~~. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M~~2~~3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~3~~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 or disposal of applicable Cyber Assets ~~that contain BES Cyber System Information~~ (except for reuse within other systems identified in the "Applicable Systems" column), ~~the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from~~ the Cyber Asset data storage media shall be sanitized or destroyed.	Examples of acceptable evidence include, but are not limited to, the following: • ~~Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or~~ • ~~Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.~~ Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal. • Records that indicate chain of custody was implemented.

~~CIP-011-2 Table R2 — BES Cyber Asset Reuse and Disposal~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~2.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence include, but are not limited to:~~ ~~• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ ~~• Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.~~

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)~~N/A~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**~~Lower~~Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented processes for BES Cyber System Information key

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						management program. (R2)
R~~2~~3	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (~~2~~3.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (~~2~~3.~~2~~1)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal. (R~~2~~3)

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	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES Cyber System Information.

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 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

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 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-011-3

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each or 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 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-011-3:

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

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

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

5. Effective Dates:

See Implementation Plan for CIP-011-3.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicability Systems" column 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-011-3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	System information pertaining to: 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	Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Examples of acceptable evidence include, but are not limited to, the following: • Documented process(es) to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Storage locations identified for housing BES Cyber System Information in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information and key management program, retention in the Physical Security Perimeter).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.4	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of acceptable evidence may include, but are not limited to, dated documentation of all of the following: • Methodology(ies) used to perform risk assessments • Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity; • Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and • Dated documentation of action plans and statuses of remediation and/or mitigation action items.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. [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-011-3 Table R2 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber Asset data storage media shall be sanitized or destroyed.	Examples of acceptable evidence include, but are not limited to, the following: • Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal. • Records that indicate chain of custody was implemented.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented processes for BES Cyber System Information key management program. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (3.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (3.1)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal. (R3)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES Cyber System Information.

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-3. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-011-3, Requirement R1

Requirement R1 was revised to include PCA and eliminate potential barriers to use cloud based services for storage of BES Cyber System Information. No changes to the VRF are necessary from the previously approved standard. The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R1

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VRF Justifications for CIP-011-3 R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in an Operations Planning time horizon to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	**Guideline 2- Consistency within a Reliability Standard** The requirement has sub-requirements and is assigned a single VRF consistent with other Requirements within the proposed standard.

VRF Justifications for CIP-011-3 R2	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective, which is to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-011-3, R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during	The Responsible Entity has not documented or implemented any processes for BES Cyber System Information protection (R2)

		storage, transit, use and disposal (Part 1.2)	

VSL Justifications for CIP-001-3, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R1 is binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-001-3, R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection.

VRF Justification for CIP-011-3, Requirement R3 (Moved from R2 to R3 in CIP-011-3)
The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R3 (Moved from R2 to R3 in CIP-011-3)
The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-2

BES Cyber System Information (BCSI)-related access management requirements were moved from CIP-004-6, Requirements R4 and R5, to CIP-011-2, Requirement R1. In addition, new requirements have been implemented to mitigate risks associated with BCSI and off-premises vendor services.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.1 Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Added requirement language for Responsible Entities to identify designated BCSI storage locations, whether physical or electronic, along with BCSI, which was already required.
CIP-011-2, Requirement R1, Part 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	CIP-011-3, Requirement R1, Part 1.2 Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use and disposal.	Established a stand-alone requirement for authorization of access to BCSI based on need, except for CIP Exceptional Circumstances. This change helps to consolidate all BCSI-related requirements under one CIP Standard. This sub-requirement was carried over from CIP-004-6, Requirement R4, Part 4.1.3. Added the lifecycle element “disposal” to the

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
		requirement to complement actions taken in CIP-011-2, Requirement R2.
CIP-004-6, Requirement R4, Part 4.1.3 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.3 Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Access to designated storage locations for BES Cyber System Information moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus changed from access to designated storage locations to access to BES Cyber System Information.
N/A	CIP-011-3, Requirement R1, Part 1.4 (NEW) Process(es) to identify, assess and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and	New CIP-011-3 requirement which is similar to the cyber security risk assessment required as part of CIP-013 Requirement R1. This new requirement is intended to focus risk analysis on potential vendors that will be hosting Responsible Entity's BCSI in the cloud.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	
CIP-004-6, Requirement R4, Part 5.3 For termination actions, revoke the individual's current 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.	CIP-011-3, Requirement R1, Part 1.5 For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Next calendar day termination actions for those with access to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus of termination actions changed from access to designated storage locations to access to BES Cyber System Information.
CIP-004-6, Requirement R4, Part 4.4 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	CIP-011-3, Requirement R1, Part 1.6 Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity	15-month entitlement reviews to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
determines are necessary for performing assigned work functions.	determines are necessary for performing assigned work functions.	Focus of verification changed from designated storage locations to BES Cyber System Information.
N/A	CIP-011-3, Requirement R2 R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection	New CIP-011-3 requirement that leverages NIST 800-57 security controls. The security of BES Cyber System Information protected by obfuscation directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.
N/A	CIP-011-3, Requirement R2, Part 2.1 (NEW) Where applicable, develop a key management program to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage	New CIP-011-3 requirement that leverages NIST 800-57 security controls. The security of BES Cyber System Information protected by obfuscation directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. Key management provides the foundation for the secure generation,

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	storage, distribution, and destruction of keys.
N/A	CIP-011-3, Requirement R2, Part 2.2 (NEW) Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	New CIP-011-3 requirement that requires implementation of controls that ensure the separation of duties and organizational independence between the programs used to restrict the ability to obtain BCSI from those programs used to restrict the ability to use BCSI.
CIP-011-2, Requirement R2, Part 2.1 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"	CIP-011-3, Requirement R3, Part 3.1 Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber	Combined CIP-011-2, Requirement R2, Part 2.1 (reuse) and CIP-011-2, Requirement R2, Part 2.2 (disposal) within the same requirement language.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Asset data storage media shall be sanitized or destroyed.	In addition, the phrase "that contain BES Cyber System Information" was removed from the requirement language effectively expanding applicability of sanitization or destruction practices to all Applicable Systems, not just those containing BCSI. This was done to align with the historical intent of CIP-007-3 Requirement R7 where reliability data was required to be sanitized as well from Cyber Assets before reuse or disposal.
CIP-011-2, Requirement R2, Part 2.2 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.	CIP-011-3, Requirement R3, Part 3.1 Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber Asset data storage media shall be sanitized or destroyed.	As above. CIP-011-2, Requirement R2, Part 2.2 was combined into CIP-011-3, Requirement R3, Part 3.1.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-011-3

December 2019

CIP-011-3 – Information Protection

Rationale for Applicability Section
Standard CIP-011 has been modified to enhance protection of BES Cyber System Information (BCSI). The modified requirements under CIP-011 will address protection of information in several facets that are discussed in this document, which include the following:

- Identification of BCSI
- Prevention of unauthorized access to BCSI
- Authorization of approved access to BCSI
- Risk assessments for BCSI not stored in the Responsible Entity's environment
- Termination of access to BCSI
- Review of access BCSI
- Key management to restrict access to BCSI
- Controls to separate duties for protecting BCSI

To provide clarity, the Applicability Systems column, which now contains BCSI, was included to associate the requirement and address the focus on protecting the BCSI regardless of the location of the BCSI. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

To address access-management-related requirements for BCSI, the related requirements from CIP-004-6 (Requirement R4, Parts 4.1.3 and 4.4, and Requirement R5, Part 5.3) have been transferred to CIP-011. This allows CIP-011 to become a more mature and easier standard to follow and update for future modifications.

Rationale for Modifications to Requirement R1, Part 1.1
Requirement R1, Part 1.1, is intended to solely identify BCSI and provide documented methods to support this identification process.

The standard drafting team (SDT) clarified the intent of addressing BCSI as opposed to the BES Cyber System (BCS) with associated applicable systems, which may contain BCSI; the Applicable Systems column

has added language to specify system information that is affiliated with High Impact and Medium Impact BES Cyber Systems and their associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Protected Cyber Assets were added to the Applicability column to ensure system information pertaining to Protected Cyber Assets is reviewed within the Responsibility Entity's information protection program subject to CIP-011 requirements, which was not previously required. Protected Cyber Assets are also applicable to CIP-011-3, Requirement R1, Parts 1.2 through 1.6, and CIP-011-3, Requirement R2, Parts 2.1 and 2.2.

Requirement language was added to Requirement R1, Part 1.1, to identify designated BCSI storage locations, whether physical or electronic. This identification should be as follows:

1) Defined as a friendly name of the electronic or physical repository (thus protecting the actual storage location); and
2) The description of the storage location (e.g., physical or electronic, off-premises or on premises).

The SDT wanted to ensure access management controls were focused on access to BCSI rather than access to BCSI designated storage locations. If a BCSI designated storage location was not identified because it does not exist, this would provide a means of accounting and clarifying this potential scenario.

The SDT has intentionally not included Low Impact BCS and their associated systems in CIP-011. Requirement R1, Part 1.1, only includes High Impact and Medium Impact BCS and their associated systems (PACS, EACMS, and PCA). The SDT also referenced Requirement R1, Part 1.1, in the Applicability column of Requirement R1, Parts 1.2 through 1.6, and Requirement R2, Parts 2.1 and 2.2, so the Responsible Entity can easily determine the applicability of those sub-requirements based on how the Responsible Entity defined and identified BCSI to satisfy Requirement R1, Part 1.1. This further clarifies there is no CIP-011 applicability to Low Impact BCS and their associated systems.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, addresses protecting and securely handling BCSI throughout its life cycle. This life cycle includes creation, use, exchange or sharing (i.e., transit), storage, and disposal. A key component of the information protection of BCSI is the secure handling of BCSI during each of these life cycle phases.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Language was added to incorporate the NERC CMEP Practice Guide where BCSI access is defined as the ability to obtain and use BCSI.

Requirement language was revised to reflect consistency with other CIP requirements as well as the current rationale for CIP-011-2, Requirement R1 (e.g., prevent unauthorized access).

Requirement language was added to include disposal as part of the BCSI life cycle. While it is assumed that disposal of BCSI is part of the BCSI life cycle, it was not previously required.

Rationale for New Requirement R1, Part 1.3
New Requirement R1, Part 1.3, was transferred from CIP-004-6, Requirement R4, Part 4.1.3, to consolidate into one Standard both BCSI protection and access authorization to BCSI.

The SDT wanted to separate the concept of protecting information via a physical device or location from protecting the information (BCSI) itself. If the focus is protection of BCSI, the device or storage location becomes less relevant. This is important when considering vendor storage as a service and security considerations regarding physical access and information moving between physical devices outside of the Responsible Entity's direct control. To accomplish this, the focus and means of protection have been shifted to address the possession and utilization of the information. Possession of BCSI addresses physical and electronic/digital controls to protect BCSI. Utilization of BCSI addresses that when BCSI is not in possession, an entity can take precautions to reasonably assure that, if BCSI is compromised from a possession aspect, the BCSI would not be able to be utilized. There are three benefits with moving in this direction:

1) There are different levels of compromise. This provides a more granular way of evaluating and reporting risk during a BCSI compromise. Before this approach, reporting a compromise or mishandling was binary and did not accurately depict risk or the actual ability of a threat actor to capitalize and exploit the information.
2) The focus is now on ensuring controls around BCSI. Physical and electronic controls now become a means to protect how information is possessed and utilized.
3) There is now the ability for the entity to address controls that are independent of possession of BCSI. This will play a significant role in leveraging technologies such as the "cloud."

The SDT also wanted to ensure backwards compatibility with the previous requirement, where feasible. Authorization for electronic and unescorted physical access and access to BCSI must still be based on necessity of the individual performing a work function. Documentation showing the authorization should still have some justification of the business need included. To ensure proper segregation of duties, the same person should still not perform access authorization and provisioning, where possible.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.4
New Requirement R1, Part 1.4, was drafted to allow Responsible Entities to implement a BCSI risk management methodology for vendors that store the Responsible Entity's BCSI and allow a risk-based approach to address the security objectives. One example of a risk-based approach is allowing Responsible Entities to develop their BCSI risk management methodology around risks posed by various vendors involved within the Responsible Entity's BCSI life cycle. This flexibility is important to account for the varying needs and characteristics of Responsible Entities and the diversity of BCSI-related environments, technologies, and risk.

The SDT recognized that CIP-013-1, Requirement R1, can be leveraged to incorporate protection of BCSI but does not currently include information protection.

This requirement includes the following three sub-requirements as a basis for implementing a BCSI risk management methodology:

1) Part 1.4.1 is included so the Responsible Entity will perform an initial risk assessment of any vendor(s) selected to store its BCSI to identify risk factors that could potentially compromise the Responsible Entity's BCSI within the vendor's environment, analyze the risk of the BCSI being compromised, and review the results of the risk analysis.
2) Part 1.4.2 is included so the Responsible Entity will review the vendor(s) that stores its BCSI at least every 15 calendar months to confirm whether the vendor(s) is still the most reliable vendor to perform that function for the Responsible Entity and the Bulk Electric System.
3) Part 1.4.3 is included so the Responsible Entity will document the results from the risk assessments performed in Parts 1.4.1 and 1.4.2 and an action plan to remediate or mitigate risks identified in the assessment.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.5
New Requirement R1, Part 1.5, was transferred from CIP-004-6, Requirement R5, Part 5.3, to consolidate into one Standard both BCSI protection and BCSI access revocation for termination actions within 24 hours.

The SDT wanted to ensure backwards compatibility with the previous requirement, where feasible. The requirement to revoke access to BCSI at the time of the termination action still includes procedures showing revocation of access to BCSI concurrent with the termination action. This requirement also still recognizes the timing of the termination action might vary depending on the circumstance.

For applicability, the SDT included Medium Impact BES Cyber Systems with this requirement regardless of whether the Medium Impact BES Cyber System had External Routable Connectivity. The SDT does not

feel that External Routable Connectivity is a determining factor for what the Responsible Entity has identified as BCSI.

Revocation of electronic access is still understood to mean a process with the result that electronic access to BCSI 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. Responsible Entities should still consider the ramifications of deleting an account might include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.6

New Requirement R1, Part 1.6, was transferred from CIP-004-6, Requirement R4, Part 4.4, to consolidate into one Standard both BCSI protection and the 15-calendar-month BCSI access review.

The SDT wanted to ensure backwards compatibility with the previous requirement, where feasible. The BCSI privilege review at least once every 15 calendar months is still in place to ensure an individual's associated privileges to BCSI are the minimum necessary to perform their work function (i.e., least privilege). This involves determining the specific roles with BCSI (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access to BCSI does not assume any specific software, and it 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 BCSI privilege review on individual accounts.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R2, Part 2.1

New Requirement R2, Part 2.1, was drafted by the SDT to require Responsible Entities to develop a key management process(es) within their information protection programs to restrict access with revocation ability. Key management provides a layer of defense against bad actors who may have the means to physically or electronically obtain BCSI but not use or modify BCSI; this has not been previously required but is needed regardless of the location or state in which the Responsible Entity's BCSI resides. The requirement language includes the minimum expectations for the key management life cycle to guide Responsible Entities while they are developing a key management program and to provide an auditable requirement for Compliance Enforcement Authorities.

The SDT identified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column has been included to accommodate this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.6.

Rationale for New Requirement R2, Part 2.2
New Requirement R2, Part 2.2, was drafted to require Responsible Entities to ensure separation of duties in the Responsible Entity's key management process(es) so, regardless of the location or state in which the Responsible Entity's BCSI resides, the risk of unauthorized access to the Responsible Entity's BCSI can be minimized. Controls must be implemented to separate the BES Cyber System Information custodial entity's duties independently from the key management duties established in Requirement R2, Part 2.1. If a Responsibility Entity is unable to implement these controls, and there is a compromise of its BCSI, the time and cost for a Responsible Entity to recover from the compromise of its BCSI could be significant to the Responsible Entity and even to the Bulk Electric System.

The SDT identified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column has been included to accommodate this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.6, and Requirement R2, Part 2.1.

Rationale for Modifications to Requirement R2, Part 2.1 (will become new Requirement R3, Part 3.1)
The SDT combined CIP-011-2, Requirement R2, Part 2.1 (reuse) and CIP-011-2, Requirement R2, Part 2.2 (disposal) within the same requirement language under CIP-011-3 Requirement R3, Part 3.1.

In addition, the phrase "that contain BES Cyber System Information" was removed from the requirement language effectively expanding applicability of sanitization or destruction practices to all Applicable Systems, not just those containing BCSI. This was done to align with the historical intent of CIP-007-3 R7 where reliability data was required to be sanitized as well from Cyber Assets before reuse or disposal.

Rationale for Retirement of CIP-011-2 Requirement R2, Part 2.2
The intent of CIP-011-2, Requirement R2, Part 2.2, which is related to BES Cyber Asset disposal, will be addressed in CIP-011-3, Requirement R3, Part 3.1, so CIP-011-2, Requirement R2, Part 2.2, is being recommended for retirement.

Technical Rationale for Reliability Standard CIP-011-2

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-011-2 standard to preserve any historical references.

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 Protection 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 of a BES Cyber Asset.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner
- Facilities[2]

Background

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2, including moving some existing CIP-004-6 Requirements to proposed CIP-011-3.

[1] See subject standards for additional information on Distribution Providers subject to the standards.
[2] See subject standards for additional information on Facilities subject to the standards.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

General Considerations

This standard will become effective 18 months following regulatory approval. The 18-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Establish and/or modify vendor relationships to establish compliance with the revised CIP-011-3 Requirements;
- Address the increased scope of the CIP-011-3 "Applicable Systems" and "Applicability" column, which has a focus on BES Cyber System Information as well as the addition of Protected Cyber Assets (PCA); and
- Develop additional sanitization programs for the life cycle of BES Cyber Systems, if necessary.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-3 – Cyber Security - Information Protection

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

CIP-004-7 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-3 – Cyber Security - Information Protection
Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2019-03 Cyber Security Supply Chain Risk Management

RELIABILITY | RESILIENCE | SECURITY






Timeline Project 2019-03

- FERC Order 850 issued October 18, 2018
  - Directed inclusion of EACMS
- NERC Cyber Security Supply Chain Risks Report published May 17, 2019
  - Recommended inclusion of PACS
- SDT Team held second meeting March 23-26, 2019
- This is the second formal posting
  - 45-day comment period, May 7 – June 22, 2020
  - 10-day ballot period, June 12 – June 22, 2020

Standards Updates

- Goal is to make minimal changes to meet the FERC Order 850 and the NERC Supply Chain report
  - Changes include adding EACMS and PACS to CIP-005, CIP-010, and CIP-013
- Coordinating with ongoing CIP projects
  - 2016-02 – Modifications to CIP Standards
  - 2019-02 – BES Cyber System Information Access Management

Draft CIP-005-7

CIP-005-6 Language (Removed)	CIP-005-7 Language (Proposed)
Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.1: Have one or more methods for ~~determining~~ detecting ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.
Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.2: Have one or more method(s) to ~~disable~~ terminate established ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.

Draft CIP-005-7

- Interactive Remote Access (IRC)
  - User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol.
  - Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP).
  - Remote access may be initiated from:
    - Cyber Assets used or owned by the Responsible Entity,
    - Cyber Assets used or owned by employees, and
    - Cyber Assets used or owned by vendors, contractors, or consultants.
  - Interactive remote access does not include system-to-system process
- Remote Access to EACMS
  - EACMS used for remote access to EACMS

Draft CIP-010-4

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS 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 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in 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: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	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.

Draft CIP-013-2

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 EACMS and 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 BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System 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 BES Cyber Systems, 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 BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated (i) ~~Interactive R~~remote A~~a~~ccess, and (ii) system-to-system remote ~~access with a vendor(s)~~.

Posting

- Draft 2 of CIP-005-7, CIP-010-4 and CIP-013-2
  - Clean and redline to last posted versions
- CIP-005-7 Summary of Changes
  - Comparison of CIP-005-6 Requirement R2.3 and R2.4 language against CIP-005-7 Requirement R3 language
- Implementation Plan
  - Modified from 12 to 18 months based on industry feedback
- Updated VRF/VSL Justification
  - VSL's updated in CIP-005-7 due to new Requirement R3
- Technical Rational for all three standards
- Draft Implementation Guidance for all three standards
  - Pending ERO approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-7 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry during the second posting of Project 2019-03, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-005-7. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. The comparison below shows the modifications from CIP-005-6 Requirement 2 Part 2.4 and Part 2.5 to CIP-005-7 Requirement 3 Part 3.1 and Part 3.2.

CIP-005-6 Language	CIP-005-7 Language
Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.1: Have one or more methods for ~~determining~~ detecting ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.
Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.2: Have one or more method(s) to ~~disable~~ terminate established ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

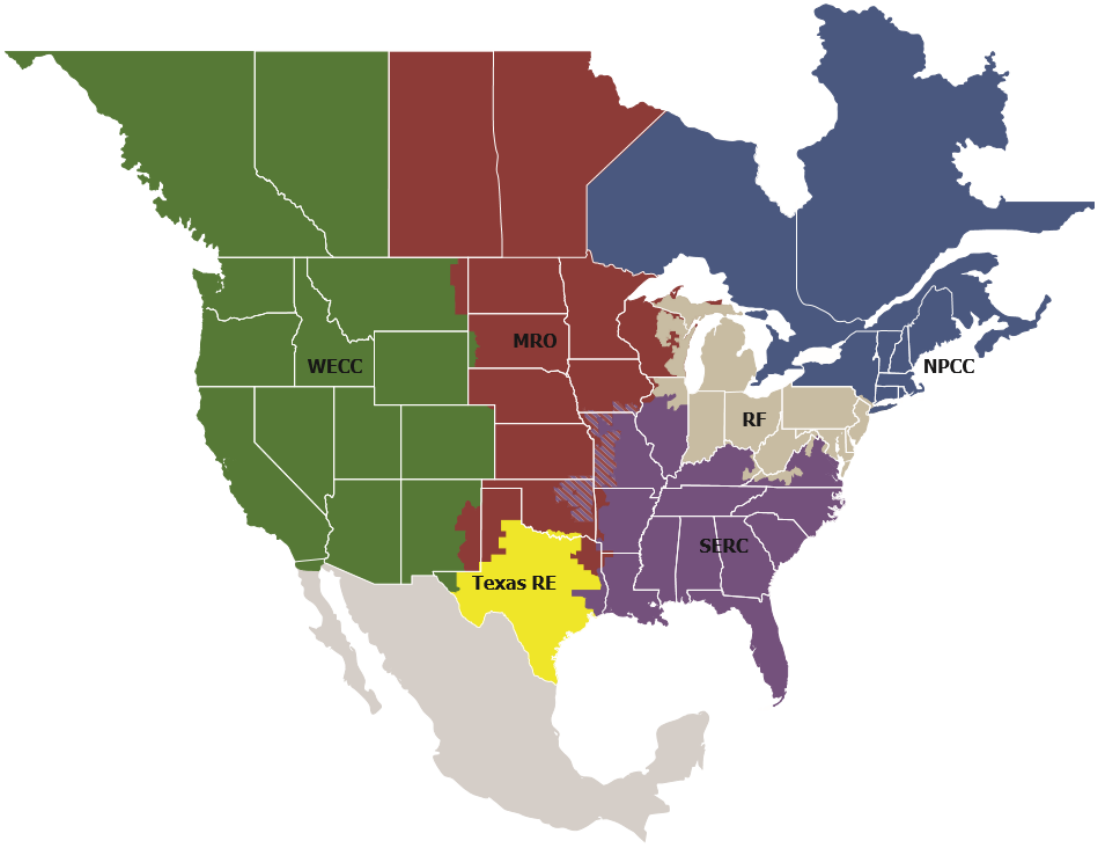
Preface iii
Introduction 4
Requirement R3 5
Implementation Guidance for CIP-005-6 7
Section 4 – Scope of Applicability of the CIP Cyber Security Standards 7
Requirement R1: 7

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management along with adding EACMs and PACs to the Applicable Systems column for Requirement parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. If an entity allows remote access to their EACMS and PACS the method for remote access would be documented and the ability to disable that remote access would be required. For example, if an entity utilizes its corporate remote access solution to allow remote access into its PACS, the entity would need to document the remote access method, and develop a process to remove such access. Removing access may be as simple as disabling a token for that user account, or suspending or deleting that user's Active Directory account.

Since EAMCs are not a requirement for remote access to other EACMs the potential of the "hall of mirrors" issue is lessened (see above example). However, if an Entity uses the same system (Intermediate System for example) for remote access into both their BES Cyber Systems and their EACMS, the process of disabling remote access becomes tricky. Since the standard requires the removal of remote access to EACMS how can that be accomplished on the EACMs itself, the "hall of mirror" effect? For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the user attempts the remote access session, the jump host will present both the Active Directory login screen as well as the multifactor access portal. The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disabled the user's ability to "access" the EACMs. The remote access user will "connect" with the EACMs however, the session will not allow "access" without the authentication methods being enabled, thus effectively not allowing remote access to that EACMS. This scenario shows a method to not allow remote access while eliminating the "hall of mirror" issue.

Where an entity strictly prohibits vendor remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations
2. An Entity could identify internal controls to periodically verify vendor remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture to provide supporting records that vendor remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.
    c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor remote access is prohibited as expected.
    d. Leveraging periodic configuration change management reviews performed in support of CIP-010-3 Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes to baseline configurations that could lead to the introduction of vendor remote access to provide additional assurance that vendor remote access is prohibited as expected.
    e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-3 Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations,

and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor remote access could be detected and reverted/revoked if established in violation of policy.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit . This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example , most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

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 ~~first~~ second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~January – March 2020~~
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

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-010-4:

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 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 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. ~~except as provided in Requirement R1, Part 1.6.~~
- **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-010-4 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-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including ~~of~~ the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	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 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 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in 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: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	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.

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 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration 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 changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

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 of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 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. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 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. (1.6)
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 the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	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-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	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-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	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-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	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-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	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-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

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

Version	Date	Action	Change Tracking
			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.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~Guidelines and Technical Basis~~

~~*Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Baseline Configuration~~

~~The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.~~

~~Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be~~

~~necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.~~

~~Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:~~

~~Asset #051028 at Substation Alpha~~

- ~~R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC~~
- ~~R1.1.2 – Not Applicable~~
- ~~R1.1.3 – Not Applicable~~
- ~~R1.1.4 – Not Applicable~~
- ~~R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823~~

~~Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.~~

~~Cyber Security Controls~~

~~The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in~~

those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007.

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a

~~plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:~~

- ~~Diagnostic test equipment;~~
- ~~Packet sniffers;~~
- ~~Equipment used for BES Cyber System maintenance;~~
- ~~Equipment used for BES Cyber System configuration; or~~
- ~~Equipment used to perform vulnerability assessments.~~

~~Transient Cyber Assets can be one of many types of devices from a specially designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.~~

~~The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.~~

~~With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would~~

negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless,

~~including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).~~

~~Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.~~

~~Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.~~

~~Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.~~

- ~~Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.~~
- ~~Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.~~

- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient

~~Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.~~

- ~~For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.~~
- ~~Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.~~
- ~~Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.~~
- ~~In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.~~
- ~~When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.~~

~~Requirement R4, Attachment 1, Section 2 – Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.~~

~~To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

~~Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.~~

- ~~Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.~~
- ~~Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.~~
- ~~Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.~~
- ~~When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.~~

~~Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

- ~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014~~

- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 – Removable Media

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

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber

~~Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.~~

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for

~~these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes~~.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT
Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-7

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

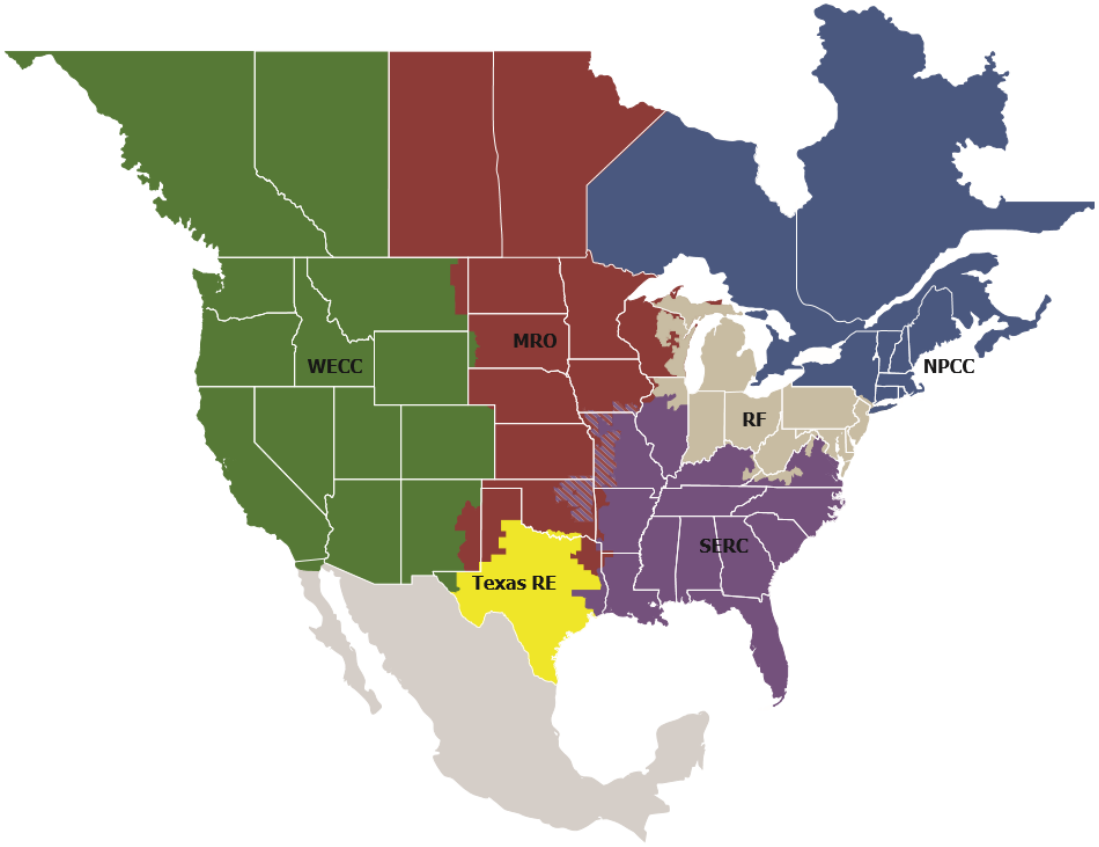
Preface iii
Introduction iv
New and Modified Terms Used in NERC Reliability Standards 5
Requirement R1 6
General Considerations for Requirement R1 6
Requirement 1 7
Requirement R2 9
General Considerations for Requirement R2 9
Requirement R3 11
Requirement 3.1 and 3.2 Vendor Remote Access Management 11
Technical Rational for Reliability Standard CIP-005-6 13
Section 4 – Scope of Applicability of the CIP Cyber Security Standards 13
Requirement R1: 13
Requirement R2: 15
Rationale: 15
Rationale for R1: 15
Rationale for R2: 16

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

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 this Section 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.

Furthermore, 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's categorization. In addition to the set of Bulk Electric System (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.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risk Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement 1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement 3.1 and 3.2 Vendor Remote Access Management

The 2019-03 SDT added Requirement 3 to contain the requirements for all types of vendor remote access management. Additionally, the SDT added EACMS and PACS to the Applicable Systems for those requirements. EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the "first line of defense within an Industry Control System (ICS) network environment". The compromise of those devices that control access management could provide an outsider the "keys to the front door" of the ESP where BES Cyber Systems reside. An intruder holding the "keys to the front door" could use those "keys" to enter the ESP or modify the access controls to allow other to bypass authorization.

Since PACS devices potentially require physical presence to exploit, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus supporting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Precedent is set in CIP-006-6 Requirement R1 Part 1.5 on the importance of PACS by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that a compromised PSP poses imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

While other Reliability Standards mitigate certain security risks relating to PACS non address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only those control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACs), however if remote access is allowed, options to determine remote access session(s) and capability to disable remote access session(s) is required.

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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 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.

Furthermore, 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'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:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

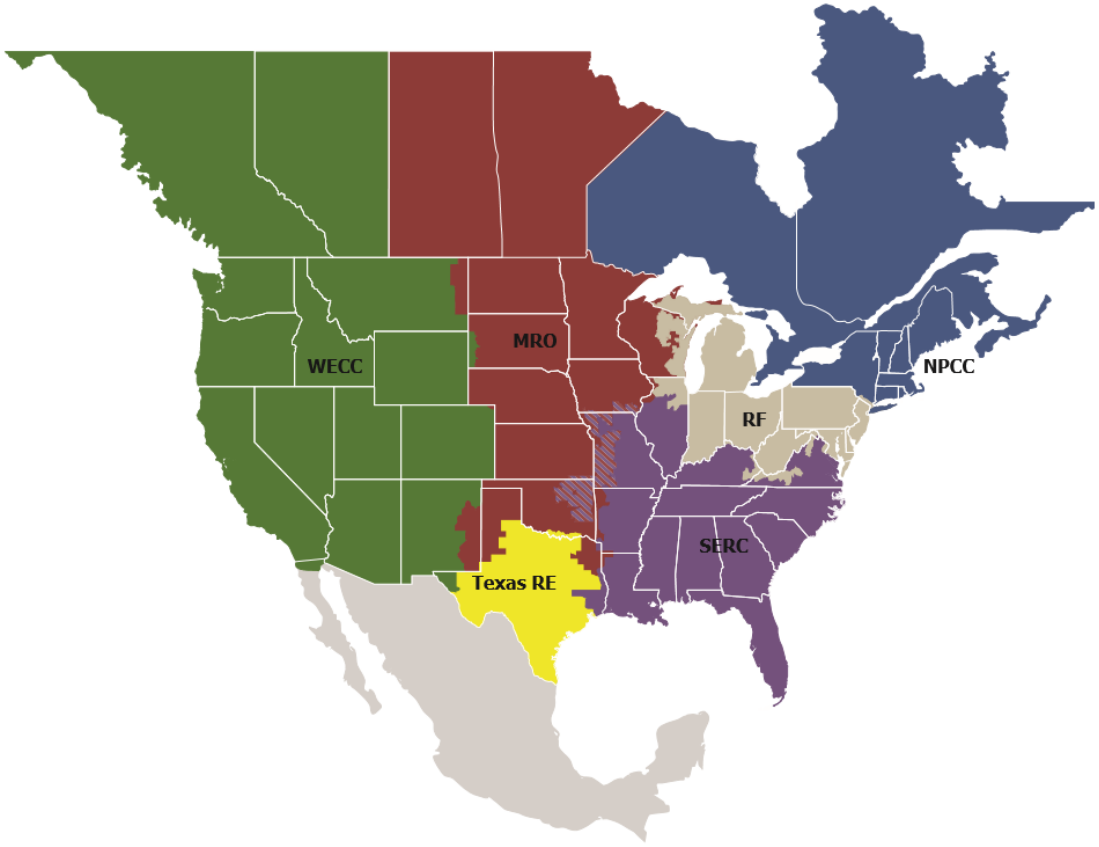
Preface iii
Introduction 4
Requirement R1 5
General Considerations for Requirement R1 5
Implementation Guidance for R1 6
Implementation Guidance for CIP-010-3 7
Section 4 – Scope of Applicability of the CIP Cyber Security Standards: 7
Requirement R1: 7
Requirement R2: 8
Requirement R3: 9
Requirement R4: 9
Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity 10
Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity 12
Requirement R4, Attachment 1, Section 3 - Removable Media 13

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

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

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

<u>Per Transient Cyber Asset Capability</u>

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[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 should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

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

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

Preface iv

Introduction v

New and Modified Terms Used on NERC Reliability Standards 6

Requirement R1 7

General Considerations for Requirement R1 7

Rationale for Requirement R1 7

Baseline Configuration 8

Cyber Security Controls 9

Test Environment 9

Software Verification 9

Requirement R2 10

Rationale for Requirement R2 10

Baseline Monitoring 10

Requirement R3 11

Rationale for Requirement R3 11

Vulnerability Assessments 11

Requirement R4 12

Rationale for Requirement R4 12

Summary of Changes 12

Transient Cyber Assets and Removable Media 12

Vulnerability Mitigation 13

Per Transient Cyber Asset Capability 13

Attachment 1 14

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity 14

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity 14

Requirement R4, Attachment 1, Section 3 - Removable Media 14

Technical Rational for Reliability Standard CIP-010-3 15

Section 4 – Scope of Applicability of the CIP Cyber Security Standards: 15

Requirement R1: 15

Requirement R2: 16

Requirement R3: 16

Requirement R4: 16

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity 18

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity 20

Requirement R4, Attachment 1, Section 3 - Removable Media 21

Rationale: 22

Rationale for Requirement R1: 22

Rationale for Requirement R2: 22

Rationale for Requirement R3: 22

Rationale for Requirement R4: 22

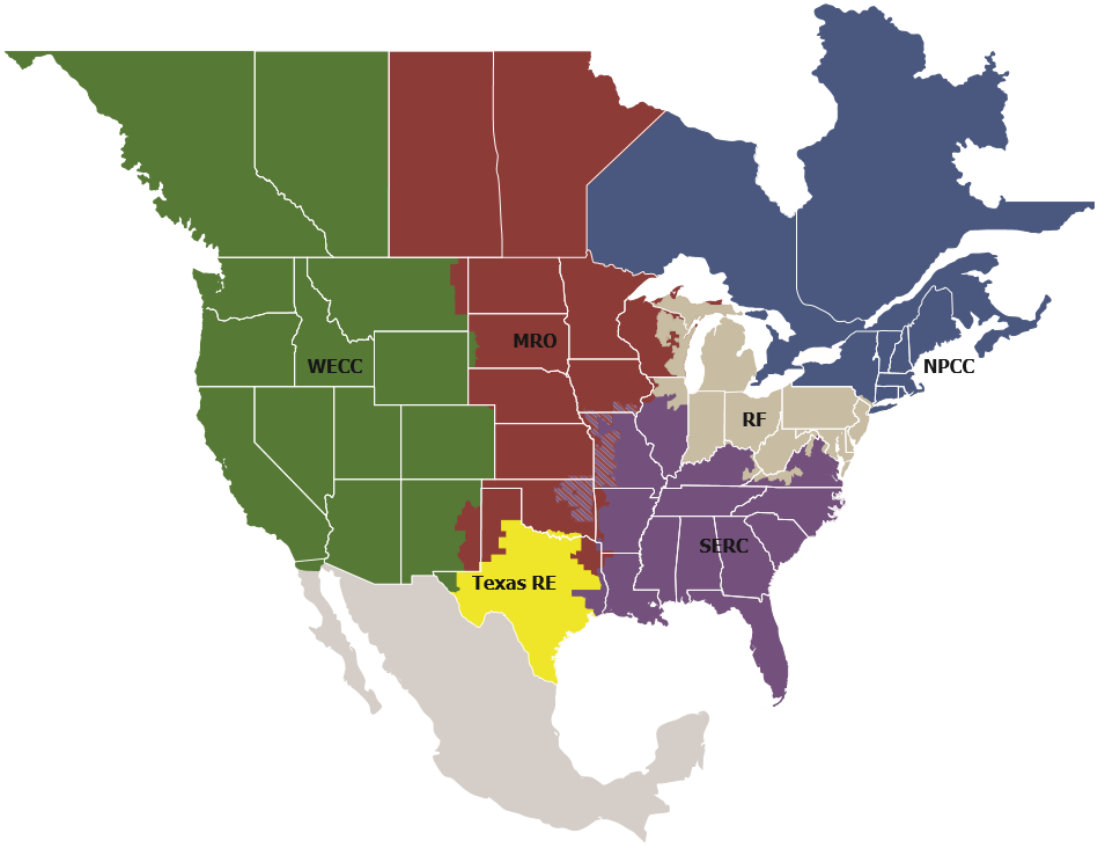
Summary of Changes: 22

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

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

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rational for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

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

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

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 configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

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 ~~first~~ second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~January – March 2020~~
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

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-010-4:

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 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 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. ~~except as provided in Requirement R1, Part 1.6.~~
- **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-010-4 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-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including ~~of~~ the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	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 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 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in 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: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	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.

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 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration 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 changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

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 of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 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. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 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. (1.6)
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 the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	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-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	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-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	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-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	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-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	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-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

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

Version	Date	Action	Change Tracking
			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.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~Guidelines and Technical Basis~~

~~*Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Baseline Configuration~~

~~The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.~~

~~Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be~~

~~necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.~~

~~Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:~~

~~Asset #051028 at Substation Alpha~~

- ~~R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC~~
- ~~R1.1.2 – Not Applicable~~
- ~~R1.1.3 – Not Applicable~~
- ~~R1.1.4 – Not Applicable~~
- ~~R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823~~

~~Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.~~

~~Cyber Security Controls~~

~~The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in~~

those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007.

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a

~~plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:~~

- ~~Diagnostic test equipment;~~
- ~~Packet sniffers;~~
- ~~Equipment used for BES Cyber System maintenance;~~
- ~~Equipment used for BES Cyber System configuration; or~~
- ~~Equipment used to perform vulnerability assessments.~~

~~Transient Cyber Assets can be one of many types of devices from a specially designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.~~

~~The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.~~

~~With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would~~

negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless,

~~including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).~~

~~Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.~~

~~Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.~~

~~Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.~~

- ~~Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.~~
- ~~Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.~~

- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient

~~Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.~~

- ~~For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.~~
- ~~Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.~~
- ~~Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.~~
- ~~In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.~~
- ~~When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.~~

~~Requirement R4, Attachment 1, Section 2 – Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.~~

~~To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

~~Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.~~

- ~~Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.~~
- ~~Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.~~
- ~~Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.~~
- ~~When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.~~

~~Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

- ~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014~~

- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 – Removable Media

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

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber

~~Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.~~

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for

~~these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes~~.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

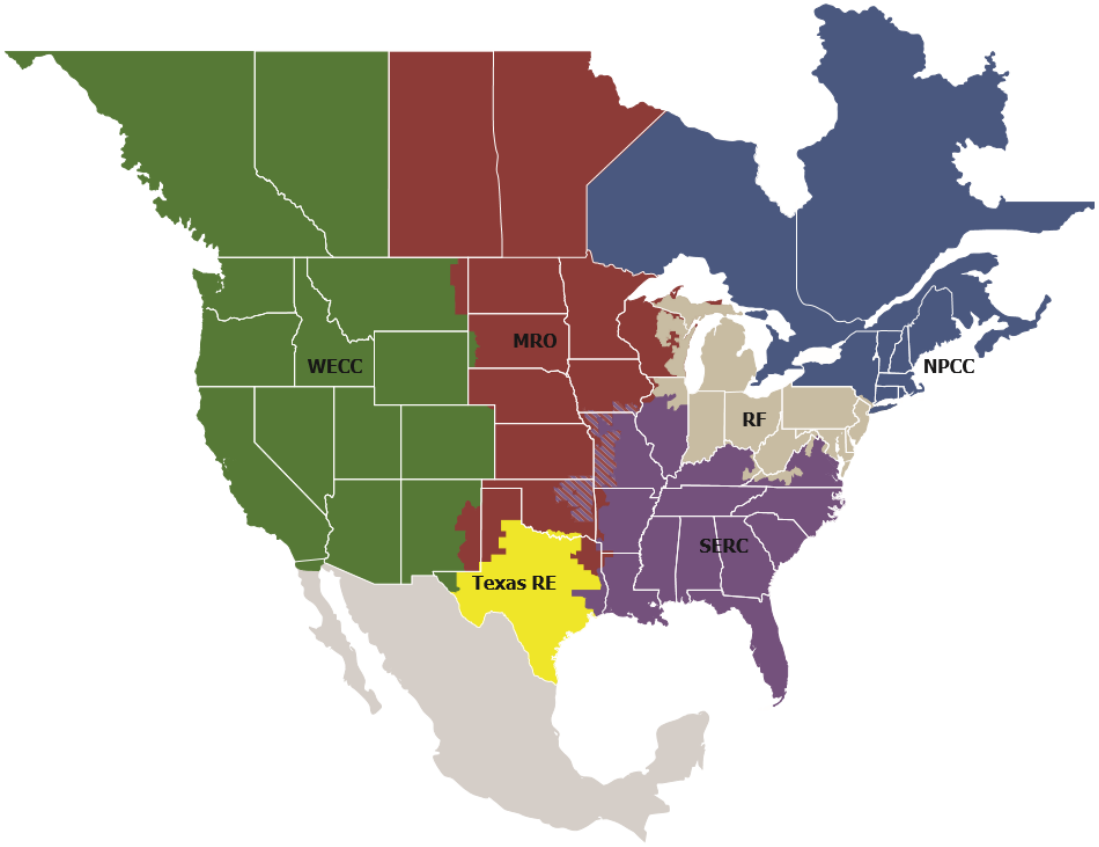
Preface iii
Introduction 4
Requirement R1 5
General Considerations for Requirement R1 5
Implementation Guidance for R1 6
Implementation Guidance for CIP-010-3 7
Section 4 – Scope of Applicability of the CIP Cyber Security Standards: 7
Requirement R1: 7
Requirement R2: 8
Requirement R3: 9
Requirement R4: 9
Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity 10
Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity 12
Requirement R4, Attachment 1, Section 3 - Removable Media 13

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

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

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

<u>Per Transient Cyber Asset Capability</u>

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[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 should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

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

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

Preface iv

Introduction v

New and Modified Terms Used on NERC Reliability Standards 6

Requirement R1 7

General Considerations for Requirement R1 7

Rationale for Requirement R1 7

Baseline Configuration 8

Cyber Security Controls 9

Test Environment 9

Software Verification 9

Requirement R2 10

Rationale for Requirement R2 10

Baseline Monitoring 10

Requirement R3 11

Rationale for Requirement R3 11

Vulnerability Assessments 11

Requirement R4 12

Rationale for Requirement R4 12

Summary of Changes 12

Transient Cyber Assets and Removable Media 12

Vulnerability Mitigation 13

Per Transient Cyber Asset Capability 13

Attachment 1 14

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity 14

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity 14

Requirement R4, Attachment 1, Section 3 - Removable Media 14

Technical Rational for Reliability Standard CIP-010-3 15

Section 4 – Scope of Applicability of the CIP Cyber Security Standards: 15

Requirement R1: 15

Requirement R2: 16

Requirement R3: 16

Requirement R4: 16

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity 18

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity 20

Requirement R4, Attachment 1, Section 3 - Removable Media 21

Rationale: 22

Rationale for Requirement R1: 22

Rationale for Requirement R2: 22

Rationale for Requirement R3: 22

Rationale for Requirement R4: 22

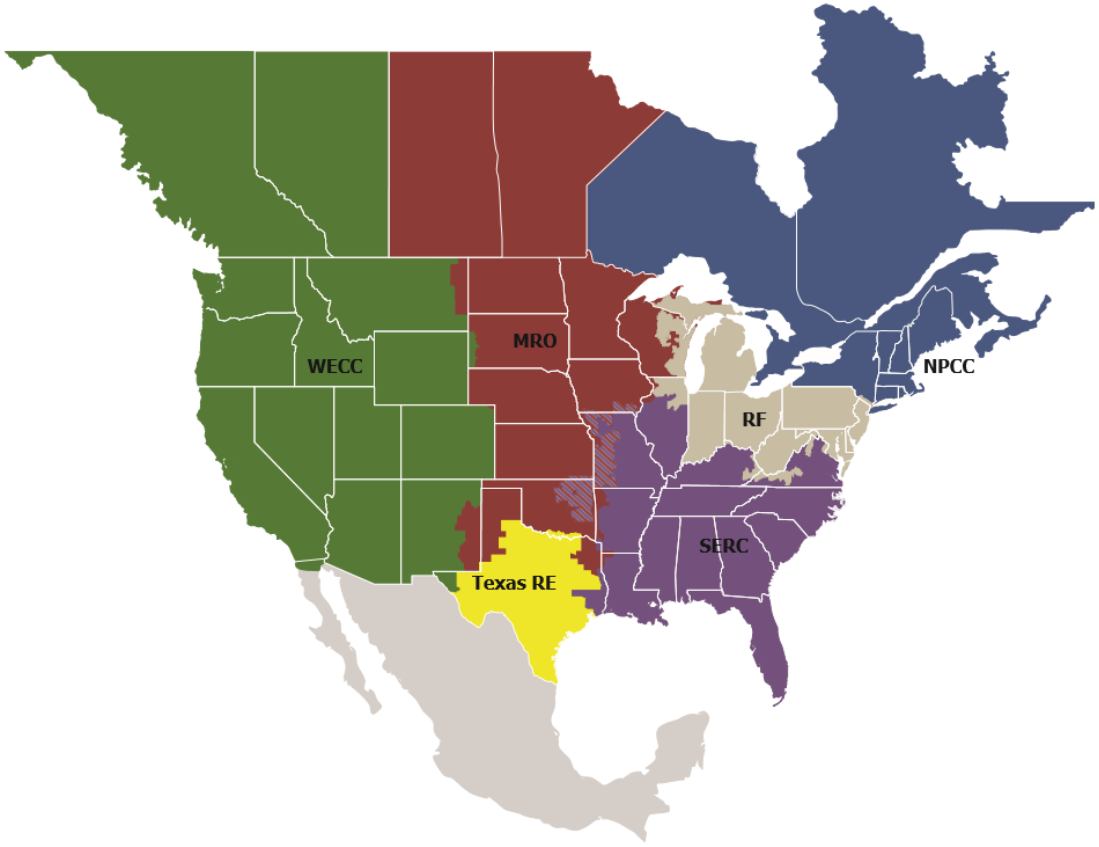
Summary of Changes: 22

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

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

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rational for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

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

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

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 configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

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 ~~first~~ second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~January – March 2020~~
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

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.

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-013-2:

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

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

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 identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See 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 EACMS and 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 BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System 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 BES Cyber Systems, 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 BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated (i) ~~Interactive R~~remote ~~A~~access, and (ii) system-to-system remote access ~~with a vendor(s)~~.

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, 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, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	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, 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, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	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, 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, as specified in 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, 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, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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 PACS, 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 Systems and their associated EACMS and PACS, 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.	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 PACS, 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 Systems and their associated EACMS and PACS, 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.	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 PACS, 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 BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	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 PACS, 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 BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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

~~Link to the Implementation Plan and other important associated documents~~None.

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.	

~~Rationale~~

~~*Note: The Rationale section has not been revised as part of the initial ballot for Project 2019-03. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

~~Requirement R1:~~

~~The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):~~

~~(1) Software integrity and authenticity;~~
~~(2) Vendor remote access;~~
~~(3) Information system planning; and~~
~~(4) Vendor risk management and procurement controls.~~

~~The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.~~

~~Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).~~

~~Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the 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); and options for mitigating these risks when planning for BES Cyber Systems.~~

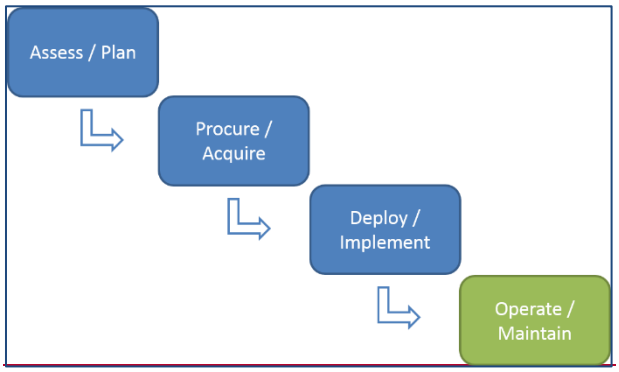
~~Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.~~

~~The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.~~

~~The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.~~

~~Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.~~

~~Notional BES Cyber System Life Cycle~~



~~Requirement R2:~~

~~The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).~~

~~Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:~~

- ~~NERC or the E-ISAC~~
- ~~ICS-CERT~~
- ~~Canadian Cyber Incident Response Centre (CCIRC)~~

~~Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT
Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-2

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

Introduction iii
Requirement R1 1
General Considerations for R1 1
Implementation Guidance for R1 2
Requirement R2 8
General Considerations for R2 8
Requirement R3 9
General Considerations for R3 9
Implementation Guidance for R3 9
References 10

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report[1] recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2~~1~~ – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[2]~~.~~ and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2~~1~~ and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2~~1~~. Responsible Entities may choose alternative approaches that better fit their situation.

[1]NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2]Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

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 EACMS and PACS. The plan(s) shall include:

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System 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 BES Cyber Systems, 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;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated (i)~~Interactive R~~remote ~~A~~access, and (ii) system-to-system remote access ~~with a vendor(s)~~.

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-~~1~~2.

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.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-~~4~~3, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

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 EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

  1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System 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).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:

- Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
- Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[3]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[4]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.

Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

[3]Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[4]For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[5].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

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;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

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;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

[5]An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.

  During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities

should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for ~~(i)~~ vendor-initiated (i) ~~Interactive~~ ~~R~~remote ~~A~~access, and (ii) system-to-system remote access ~~with a vendor(s)~~.*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

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.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-2~~1~~. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2~~1~~.

Requirement R3

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.

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) "Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation"
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-2

May 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

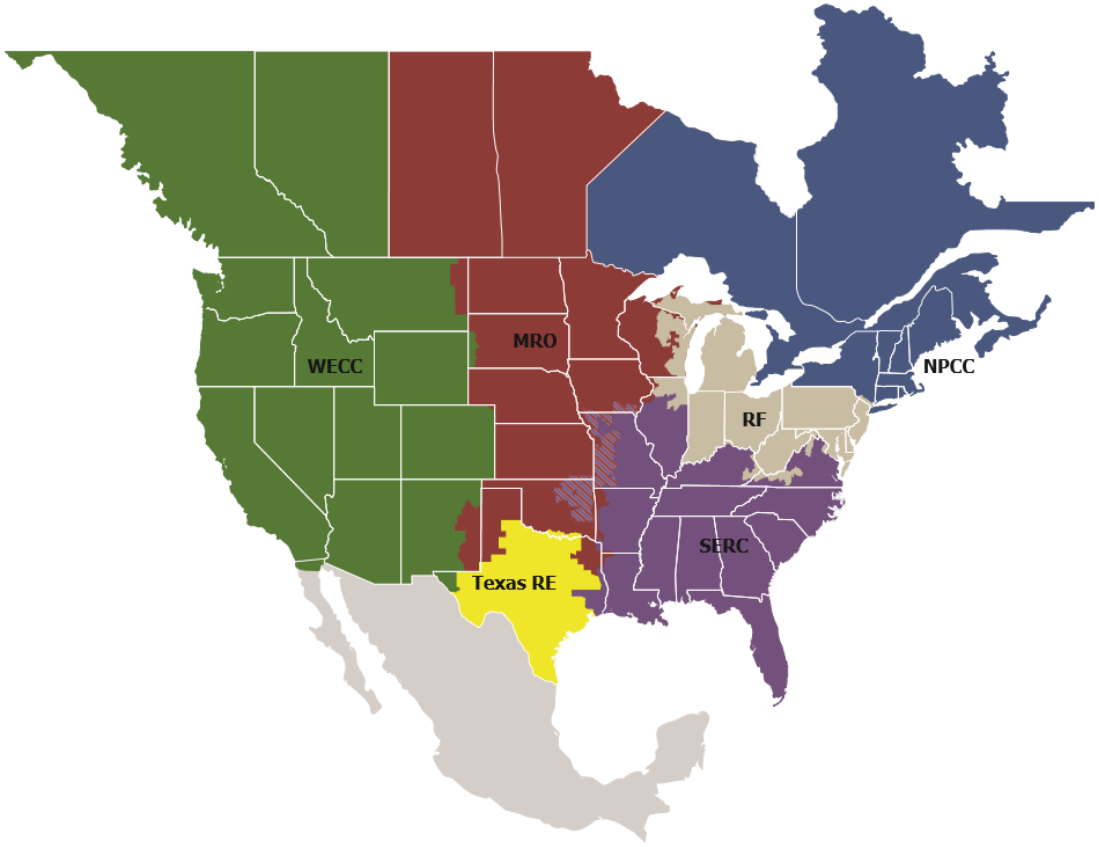
Preface iii
Introduction iv
New and Modified Terms Used on NERC Reliability Standards 5
Requirement R1 6
General Considerations for Requirement R1 6
Rational for Requirement 1 7
Requirement R2 9
General Considerations for Requirement R2 9
Technical Rational for Reliability Standard CIP-013-1 10

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the 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); and options for mitigating these risks when planning for BES Cyber Systems.

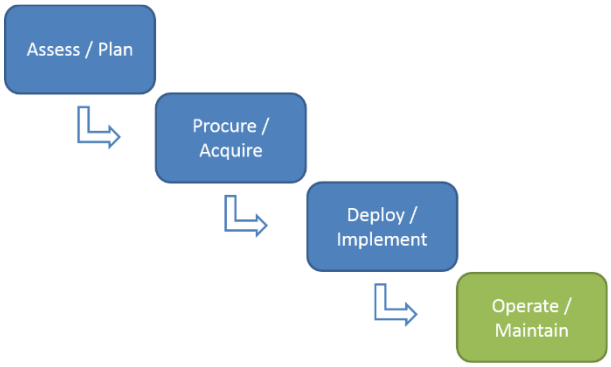
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2

General Considerations for Requirement R2

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the 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); and options for mitigating these risks when planning for BES Cyber Systems.

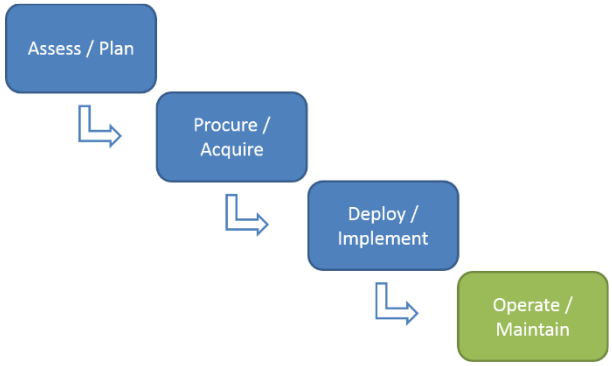
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement~~s~~ R3~~2.4 and R2.5~~ and CIP-010-4 Requirement R1.6 ~~and~~ to include EACMS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirement~~s~~ R3~~2.4 and R2.5~~ and CIP-010-4 Requirement R1.6 ~~and~~ to include PACS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6.

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

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

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-005-7, Requirement R1

The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirement R1

The VSL did not change from the FERC-approved CIP-005-6 Reliability Standard.

VRF Justification for CIP-005-7, Requirement R2

The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirement R2

The VSL is explained in the following pages.

VRF Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VSL Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VRF Justification for CIP-010-4

The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4

The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2, Requirement R1

The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R1
The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirement.

VRF Justification for CIP-013-2, Requirement R2
The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R2
The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirement.

VRF Justification for CIP-013-2, Requirement R3
The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R3
The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSLs for CIP-005-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	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;~~OR~~ ~~The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system to~~	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; ~~OR~~ ~~The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and~~

		~~system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).~~	~~system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).~~

VSL Justifications for CIP-005-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from the FERC approved CIP-005-6 Reliability Standard, with the following exceptions. In the high and severe VSL, the second levels are removed because Requirement R2 Part 2.4 and Part 2.5 have been removed from the standard language. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3)	The Responsible Entity did not have a method for detecting vendor-initiated remote access sessions for PACS but had method(s) as required by Part 3.1 for other applicable systems types (3.1). OR The Responsible Entity did not have a method to terminate established vendor-initiated	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by 3.1 for PACS but did not have a method for detecting vendor-initiated remote access sessions for other applicable system(s) types (3.1). OR	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3). OR The Responsible Entity had methods as required by 3.1 and 3.2 for PACS but did not have any

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
	remote access sessions for PACS but had method(s) as required by Part 3.2 for other applicable systems types (3.2).	The Responsible Entity had method(s) as required by 3.2 for PACS but did not have a method to terminate established vendor-initiated remote access sessions for other applicable system(s) types (3.2). OR The Responsible Entity did not have method(s) as required by Part 3.1 or Part 3.2 for PACS and one or more other applicable systems type(s). (3.1 or 3.2) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 for PACS but had method(s) as required by Parts 3.1 and 3.2 other applicable systems types. OR The Responsible Entity did not have method(s) as required by Parts 3.1 and 3.2 for PACS and one or more other applicable system types. (3.1 and 3.2)	methods as required by Parts 3.1 and 3.2 for other applicable system types (R3).

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs are based on the newly formed CIP-005-7 Requirement R3 which are modified from CIP-005-6 Requirement R2 Part 2.4 and Part 2.5. The Requirement R3 were modelled after the original CIP-005-6 Requirement R2 VSL's with the addition of PACS as an applicable system at a lower level than the other applicable system types listed in Requirement R3 Part 3.1 and Part 3.2.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Medium is being proposed for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirement R2 which Requirement R3 is modified from.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	A VRF of Medium is consistent with Reliability Standard CIP-005-7 Requirement R3 which addresses Remote Access Management.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium is consistent with the NERC VRF Definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher-risk reliability objective with a lesser- risk reliability objective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - 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.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18~~2~~ months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18~~2~~ months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6. The Implementation Plan associated with CIP-002-6 provides as follows~~The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5 shall apply to CIP-002-6. The Implementation Plan associated with CIP-002-5 provided as follows with respect to planned and unplanned changes (with conforming changes to the version numbers of the standard)~~:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber

System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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:	5/9/2019		
SAR Requester			
Name:	Alison Mackellar		
Organization:	North American Generator Forum (NAGF)		
Telephone:	630-657-2817	Email:	alison.mackellar@exeloncorp.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?):			
PRC-005-6 needs to be revised to provide clear guidance on the scope of applicability to Automatic Voltage Regulator (AVR) protective functions. Without clear applicability the industry is struggling with how to implement PRC-005-6 and what testing is acceptable to meet the required maintenance activities prescribed by PRC-005-6.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Provide clear, unambiguous applicability of PRC-005-6 to AVR protective functions and the specificity needed for the industry to consistently identify and implement the required maintenance activities.			
Project Scope (Define the parameters of the proposed project):			
Revise PRC-005-6 to clearly define the applicability of Protection Systems associated with AVR protective functions. In addition, revise the PRC-005-6 Supplementary Reference and FAQ to provide additional guidance related to AVR protective functions and acceptable methods of testing to meet PRC-005-6 required maintenance activities.			

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 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):
1. Revise PRC-005-6 to add a new section under Facilities to clearly delineate the applicability of Protection Systems associated with AVR protective functions. This new section needs to clearly limit the scope of the AVR protective functions to those elements that open a breaker directly or via lockout or tripping auxiliary relays. 2. Revise the PRC-005-6 Supplementary Reference and FAQ Section 15 to provide a more detailed description of the applicability of AVR protective functions and to provide acceptable methods of testing to meet PRC-005-6 required maintenance activities.
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):
Only applicable to a Generator Owner that owns a synchronous generating unit with an installed digital AVR
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)
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 this SAR and have communicated the issue in advance to NERC.
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)?
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.

[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.

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
e.g., NPCC	None

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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:	Modification to PER-003-2		
Date Submitted:	09 July2019		
SAR Requester			
Name:	Personnel Certification and Governance Committee (Chair – Mike Anderson)		
Organization:	NERC		
Telephone:	(614) 413-2311	Email:	mcanderson@aep.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?):			
Enhanced BES Reliability			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Referencing the PCGC's "One System Operator Certification credential" whitepaper, all System Operators would hold the same Certification credential. This better serves reliability by ensuring all System Operators, regardless of their company's registration or credential of choice, have the same base knowledge. This knowledge is demonstrated through the System Operator Certification process.			
Project Scope (Define the parameters of the proposed project):			
Modify Reliability Standard PER-003-2 by consolidating four separate System Operation Certification credentials into a single credential. Team will develop the implementation plan timeline in coordination with the PCGC transition plan. ~~Modification of PER-003-2 through the Standards Development Process~~			

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 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):
Modify Reliability Standard PER-003-2 by consolidating four separate System Operation Certification credentials into a single credential. ~~Revise PER-003-2 to address one credential is required, not the current four credentials.~~ PER-005 did not exist at the inception of system operator certification. PER-003-2 is a personal certification of minimal knowledge and skills; whereas PER-005 addresses more specific reliability related tasks for entity qualifications/requirements. The team will consider the relationship between PER-003-2 and PER-005-2 as well as the relationship between PER-003-2 and the System Operator Certification Program Manual. ~~To address any potential gaps concerning the misconception of applicable areas of competency, please consider making a stronger tie between the revised PER-003-2 to PER-005. It is still important to maintain the independence of each Standard.~~
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Minimal cost impact to industry as bundled in the PCGC's budget recovered through existing exam and renewal fees.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
N/A
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, Transmission Operator, Balancing Authority
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.
Industry circulated "One Credential" whitepaper and associated comments/responses from the PCGC
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)?
None
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

[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.

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
e.g., NPCC	

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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:	Modification to PER-003-2		
Date Submitted:	09 July2019		
SAR Requester			
Name:	Personnel Certification and Governance Committee (Chair – Mike Anderson)		
Organization:	NERC		
Telephone:	(614) 413-2311	Email:	mcanderson@aep.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?):			
Enhanced BES Reliability			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Referencing the PCGC's "One System Operator Certification credential" whitepaper, all System Operators would hold the same Certification credential. This better serves reliability by ensuring all System Operators, regardless of their company's registration or credential of choice, have the same base knowledge. This knowledge is demonstrated through the System Operator Certification process.			
Project Scope (Define the parameters of the proposed project):			
Modify Reliability Standard PER-003-2 by consolidating four separate System Operation Certification credentials into a single credential. Team will develop the implementation plan timeline in coordination with the PCGC transition plan.			

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 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):
Modify Reliability Standard PER-003-2 by consolidating four separate System Operation Certification credentials into a single credential. PER-005 did not exist at the inception of system operator certification. PER-003-2 is a personal certification of minimal knowledge and skills; whereas PER-005 addresses more specific reliability related tasks for entity qualifications/requirements. The team will consider the relationship between PER-003-2 and PER-005-2 as well as the relationship between PER-003-2 and the System Operator Certification Program Manual.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Minimal cost impact to industry as bundled in the PCGC's budget recovered through existing exam and renewal fees.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
N/A
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, Transmission Operator, Balancing Authority
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.
Industry circulated "One Credential" whitepaper and associated comments/responses from the PCGC
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)?
None
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

[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.

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
e.g., NPCC	

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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:	~~Extreme~~ Cold Weather Preparedness and Communication Requirements between Functional Entities		
Date Submitted:	September 20, 2019		
SAR Requester			
Name:	Michael Desselle, VP Process Integrity/Chief Compliance and Administrative Officer		
Organization:	Southwest Power Pool, Inc.		
Telephone:	(501) 614-3206	Email:	mdesselle@spp.org

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?):
To enhance the reliability of the BES during cold weather events by ensuring Generator Owners, Generator Operators, Reliability Coordinators, and Balancing Authorities prepare for ~~extreme~~ cold weather conditions. Additonally, to ensure communications between functional entities of cold weather impacts to generator unit availability.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
To ensure optimal reliability by preparing generation for ~~extreme~~ cold weather performance and ensure situational awareness in both planning and operations by applicable registered entities.

Requested information
Project Scope (Define the parameters of the proposed project):
The project scope will address Recommendation 1 in the 2019 FERC and NERC Staff Report: The South-Central United States Cold Weather BES Event of January 17, 2018; and will include the development of ~~a~~ new or revised NERC Reliability Standard to consider such activities as winterization activities on BES generating units, winter-specific and plant-specific operator awareness training, and processes to ensure situational awareness for the registered functions.
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):
Technical justification can be found in the findings and recommendations contained in the *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 at the following link: https://www.ferc.gov/legal/staff-reports/2019/07-18-19-ferc-nerc-report.pdf. The deliverable will be new or revised Reliability Standards, as appropriate, to promote reliability of the BES during ~~extreme~~ cold weather and to ensure that cold weather performance plans for BES generating units are developed, implemented, and communicated in order to maintain BES generating unit availability within performance capabilities or operating limitations. 1. Generator Owner/Generator Operator[2] develops and implements cold weather preparedness ~~winterization~~ plans, procedures, and ~~winter-specific and plant-specific operator~~ awareness training based on factors such as geographical location and plant configurations. ~~Additional e~~Elements ~~to~~ for consideration may include: a. ~~Generating unit availability~~ The need for accurate cold weather temperature design specifications or historical demonstrated performance, and operating limitations during cold weather; ~~b. Parameters around operating temperatures;~~ ~~c.~~b. Implementing freeze protection measures ~~and technologies~~; ~~d.~~c. Performing periodic adequate maintenance and inspection of freeze protection measures ~~and technologies~~; and

Formatted: Indent: Left: 0.75", No bullets or numbering

[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] The term Generator Owner/Generator Operator used throughout the SAR is a used as a broad categorization rather than a definitive requirement for both entities. The intention is for the Standard Drafting Team to determine the appropriate responsible entity based on the NERC Glossary of Terms and functional obligations defined in the standards.

Requested information
~~e.~~d. Providing adcance notification (when available) of curtailments of natural gas to a ~~Ensuring gas fueled~~BES generating unit~~'~~s~~'~~ Reliability Coordinator and Balancing Authority ~~are provided notification of firm transportation capacity for natural gas supply~~. 2. Generator Owner/Generator Operator communicates with the Balancing Authorities~~,~~ ~~and~~ Reliability Coordinators, and Transmission Operators the ~~associated parameters for~~BES generating unit's associated design specification or historical demonstrated performance, and operating limitations during ~~availability for extreme~~ cold weather~~,~~ ~~performance~~ including as required by deliverable 1d. 3. Generator Owners/Generator Operator communicates with the Balancing Authorities~~,~~ ~~and~~ Reliability Coordinators, and Transmission Operator when local forecasted cold weather conditions are expected to ~~temperatures are forecasted within the determined~~ limit BES generating unit performance or BES generating unit availability~~ies~~.~~,~~ ~~expected availability of the generating units for the appropriate next day operating horizon.~~ 4. Reliability Coordinators, Balancing Authority, and Transmission Operator incoproate the use of the data, as communicated in deliverable #2 and #3 above, ~~use of the information provided by the Generator Owner/Generator Operator~~ to perform their respective Operational Planning Analysis, ~~and~~ develop its Operating Plans, or determine the expected availability ~~and~~ of contingency reserves for the appropriate next day operating horizon.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown. However, a question should be asked during the SAR comment period to ensure all aspects are considered.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Each BES facility considered here may have numerous unique characteristics based on factors such as construction, technical configuration, geographic differences, etc. The substantive differences may require flexibility for each generation resource to develop the appropriate plans to implement during ~~extreme~~ cold weather events.

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):
Balancing Authority, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator
Do you know of any consensus building activities[3] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 was publicly noticed and shared with regulators and industry.
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)?
In implementing the project scope, the preference is for the Standards Drafting Team to utilize and revise, to the extent possible, the current Operating and Planning suite of mandatory Reliability Standards subject to enforcement and create a new standard only if necessary and appropriate.The proposed deliverables, as well as other proposed requirements applicable to Generator Owners, Generator Operators, Balancing Authorities and Reliability Coordinators, that may result from this project ~~should~~ must be reviewed to ensure any conflicts or overlap with current requirements are mitigated. For example, IRO-010-2, ~~and~~ TOP-003-3, and EOP-011 may address some of these aspects already. These standards require the Reliability Coordinator (IRO-010-2) and Balancing Authority (TOP-003-3) to maintain documented data specifications that include a list of data and information they need to support the Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Applicable Registered Entities, which include Transmission Operators, Balancing Authorities, Generator Operators, Generator Owners, Transmission Owners, and Distribution Providers, are then required to provide the data per the data specifications. Additionally, EOP-011 includes consideration of generator management and extreme weather conditions.
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.

[3] 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
A number of recommendations contained in the following FERC and NERC reports could be utilized by the standard drafting team: *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 *Polar Vortex Review*, September 2014 *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011: Causes and Recommendations,* August 2011 *Reliability Guideline: Generating Unit Winter Weather Readiness – Current Industry Practices.*

Formatted: Font: Italic

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

Market Interface Principles	
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	

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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:	Cold Weather Preparedness and Communication Requirements between Functional Entities		
Date Submitted:	September 20, 2019		
SAR Requester			
Name:	Michael Desselle, VP Process Integrity/Chief Compliance and Administrative Officer		
Organization:	Southwest Power Pool, Inc.		
Telephone:	(501) 614-3206	Email:	mdesselle@spp.org

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?):
To enhance the reliability of the BES during cold weather events by ensuring Generator Owners, Generator Operators, Reliability Coordinators, and Balancing Authorities prepare for cold weather conditions. Additonally, to ensure communications between functional entities of ~~all ambient~~ cold weather impacts to generator unit availability.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
To ensure optimal reliability by preparing generation for cold weather performance and ensure situational awareness in both planning and operations by applicable registered entities.

Requested information
Project Scope (Define the parameters of the proposed project):
The project scope will address Recommendation 1 in the 2019 FERC and NERC Staff Report: The South-Central United States Cold Weather BES Event of January 17, 2018; and will include the development of new or revised NERC Reliability Standards to consider such activities as winterization activities on BES generating units, winter-specific and plant-specific operator awareness training, and processes to ensure situational awareness for the registered functions.
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):
Technical justification can be found in the findings and recommendations contained in the *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 at the following link: https://www.ferc.gov/legal/staff-reports/2019/07-18-19-ferc-nerc-report.pdf. The deliverable will be new or revised Reliability Standards, as appropriate, to promote reliability of the BES during cold weather and ~~maximize~~ to ensure that cold weather performance plans for BES generating units are developed, implemented, and communicated in order to maintain BES generating unit availability within performance capabilities or operating limiations. 1. Generator Owner/Generator Operator[2] develops and implements cold weather preparedness plans, procedures, and awareness training based on factors such as geographical location and plant configurations~~. Elements for consideration~~ may include: a. The need for accurate cold weather temperature design specifications or historical demonstrated performance and operating limitations during cold weather ~~A generating unit's historical demonstrated performance and operating limitations during ambient cold weather~~; b. Implementing freeze protection measures; c. Performing periodic adequate maintenance and inspection of freeze protection measures; and d. Providing advance notification (when available) of curtailments of natural gas to a ~~supply to a gas-fueled~~ BES generating unit's Reliability Coordinator and Balancing Authority.

[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] The term Generator Owner/Generator Operator used throughout the SAR is a used as a broad categorization rather than a definitive requirement for both entities. The intention is for the Standard Drafting Team to determine the appropriate responsible entity based on the NERC Glossary of Terms and functional obligations defined in the standards.

Requested information
2. Generator Owner/Generator Operator communicates with the Balancing Authorities, ~~and~~ Reliability Coordinators, and Transmission Operators the BES generating unit's associated design specification or historical demonstrated performance and operating limitations during ~~ambient~~ cold weather, including as required by deliverable 1d. 3. Generator Owner/Generator Operator communicates with the Balancing Authorities, ~~and~~ Reliability Coordinators, and Transmission Operator when local forecasted ~~ambient~~ cold weather conditions ~~(including, but not limited to, cold weather temperatures)~~ are expected to ~~impact generating unit performance or~~limit BES generating unit performance or BES generating unit availability. ~~for the appropriate next day operating horizon.~~ 4. Reliability Coordinators, ~~and~~ Balancing Authorities, and Transmission Operator incorporates ~~use of~~ the data, as communicated in ~~generating unit performance and availability provided through~~ deliverable #2 and #3 above, to perform their respective Operational Planning Analysis, develop its Operating Plans, or determine the expected availability ~~and~~ of contingency reserves for the appropriate next day operating horizon.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown. However, a question should be asked during the SAR comment period to ensure all aspects are considered.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Each BES facility considered here may have numerous unique characteristics based on factors such as construction, technical configuration, geographic differences, etc. The substantive differences may require flexibility for each generation resource to develop the appropriate plans to implement during cold weather events.
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):
Balancing Authority, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator

Requested information
Do you know of any consensus building activities[3] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 was publicly noticed and shared with regulators and industry.
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)?
In implementing the project scope, the preference is for the Standards Drafting Team to utilize and revise, to the extent possible, the current Operating and Planning Suite of mandatory Reliability Standards subject to enforcement and create a new standard only if necessary and appropriate.The proposed deliverables, as well as other proposed requirements applicable to Generator Owners, Generator Operators, Balancing Authorities and Reliability Coordinators, that may result from this project ~~should~~ must be reviewed to ensure any conflicts or overlap with current requirements are mitigated. For example, IRO-010-2, ~~and~~ TOP-003-3, and EOP-011 may address some of these aspects already. These standards require the Reliability Coordinator (IRO-010-2) and Balancing Authority (TOP-003-3) to maintain documented data specifications that include a list of data and information they need to support the Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Applicable Registered Entities, which include Transmission Operators, Balancing Authorities, Generator Operators, Generator Owners, Transmission Owners, and Distribution Providers, are then required to provide the data per the data specifications. Additonally, EOP-011 includes consideration of generator management and extreme weather conditions. ~~The Operating and Planning suite of standards will be considered for this project.~~
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.
A number of recommendations contained in the following FERC and NERC reports could be utilized by the standard drafting team: *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019

[3] 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
Polar Vortex Review, September 2014 *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011: Causes and Recommendations,* August 2011 *Reliability Guideline: Generating Unit Winter Weather Readiness – Current Industry Practices.* *Reliability Guideline: Generating Unit Winter Weather Readiness – Current Industry Practices.*

Formatted: Font: Italic

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	Yes

Market Interface Principles	
access commercially non-sensitive information that is required for compliance with reliability standards.	

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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:	Cold Weather Preparedness and Communication Requirements between Functional Entities		
Date Submitted:	September 20, 2019		
SAR Requester			
Name:	Michael Desselle, VP Process Integrity/Chief Compliance and Administrative Officer		
Organization:	Southwest Power Pool, Inc.		
Telephone:	(501) 614-3206	Email:	mdesselle@spp.org

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?):

To enhance the reliability of the BES during cold weather events by ensuring Generator Owners, Generator Operators, Reliability Coordinators, and Balancing Authorities prepare for cold weather conditions. Additonally, to ensure communications between functional entities of cold weather impacts to generator unit availability.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

To ensure optimal reliability by preparing generation for cold weather performance and ensure situational awareness in both planning and operations by applicable registered entities.

Requested information
Project Scope (Define the parameters of the proposed project):
The project scope will address Recommendation 1 in the 2019 FERC and NERC Staff Report: The South-Central United States Cold Weather BES Event of January 17, 2018; and will include the development of new or revised NERC Reliability Standards to consider such activities as winterization activities on BES generating units, winter-specific and plant-specific operator awareness training, and processes to ensure situational awareness for the registered functions.
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):
Technical justification can be found in the findings and recommendations contained in the *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 at the following link: https://www.ferc.gov/legal/staff-reports/2019/07-18-19-ferc-nerc-report.pdf. The deliverable will be new or revised Reliability Standards, as appropriate, to promote reliability of the BES during cold weather and to ensure that cold weather performance plans for BES generating units are developed, implemented, and communicated in order to maintain BES generating unit availability within performance capabilities or operating limiations. 1. Generator Owner/Generator Operator[2] develops and implements cold weather preparedness plans, procedures, and awareness training based on factors such as geographical location and plant configurations may include: a. The need for accurate cold weather temperature design specifications or historical demonstrated performance and operating limitations during cold weather ; b. Implementing freeze protection measures; c. Performing periodic adequate maintenance and inspection of freeze protection measures; and d. Providing advance notification (when available) of curtailments of natural gas to a BES generating unit's Reliability Coordinator and Balancing Authority. 2. Generator Owner/Generator Operator communicates with the Balancing Authorities, Reliability Coordinators, and Transmission Operators the BES generating unit's associated design

[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] The term Generator Owner/Generator Operator used throughout the SAR is a used as a broad categorization rather than a definitive requirement for both entities. The intention is for the Standard Drafting Team to determine the appropriate responsible entity based on the NERC Glossary of Terms and functional obligations defined in the standards.

Requested information
specification or historical demonstrated performance and operating limitations during cold weather, including as required by deliverable 1d. 3. Generator Owner/Generator Operator communicates with the Balancing Authorities, Reliability Coordinators, and Transmission Operator when local forecasted cold weather conditions are expected to limit BES generating unit performance or BES generating unit availability. 4. Reliability Coordinators, Balancing Authorities, and Transmission Operator incorporates the data, as communicated in deliverable #2 and #3 above, to perform their respective Operational Planning Analysis, develop its Operating Plans, or determine the expected availability of contingency reserves for the appropriate next day operating horizon.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown. However, a question should be asked during the SAR comment period to ensure all aspects are considered.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Each BES facility considered here may have numerous unique characteristics based on factors such as construction, technical configuration, geographic differences, etc. The substantive differences may require flexibility for each generation resource to develop the appropriate plans to implement during cold weather events.
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):
Balancing Authority, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator
Do you know of any consensus building activities[3] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.

[3] 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
The *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 was publicly noticed and shared with regulators and industry.
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)?
In implementing the project scope, the preference is for the Standards Drafting Team to utilize and revise, to the extent possible, the current Operating and Planning Suite of mandatory Reliability Standards subject to enforcement and create a new standard only if necessary and appropriate.The proposed deliverables, as well as other proposed requirements applicable to Generator Owners, Generator Operators, Balancing Authorities and Reliability Coordinators, that may result from this project must be reviewed to ensure any conflicts or overlap with current requirements are mitigated. For example, IRO-010-2, TOP-003-3, and EOP-011 may address some of these aspects already. These standards require the Reliability Coordinator (IRO-010-2) and Balancing Authority (TOP-003-3) to maintain documented data specifications that include a list of data and information they need to support the Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Applicable Registered Entities, which include Transmission Operators, Balancing Authorities, Generator Operators, Generator Owners, Transmission Owners, and Distribution Providers, are then required to provide the data per the data specifications. Additonally, EOP-011 includes consideration of generator management and extreme weather conditions.
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.
A number of recommendations contained in the following FERC and NERC reports could be utilized by the standard drafting team: *2019 FERC and NERC Staff Report: The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018*, July 2019 *Polar Vortex Review*, September 2014 *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011: Causes and Recommendations,* August 2011 *Reliability Guideline: Generating Unit Winter Weather Readiness – Current Industry Practices.*

Requested information
Reliability Guideline: Generating Unit Winter Weather Readiness – Current Industry Practices.

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	

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

A. Introduction

1. **Title:** Balancing Authority Control

2. **Number:** BAL-005-1

3. **Purpose:** This standard establishes requirements for acquiring data necessary to calculate Reporting Area Control Error (Reporting ACE). The standard also specifies a minimum periodicity, accuracy, and availability requirement for acquisition of the data and for providing the information to the System Operator.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

Effective Date: See Implementation Plan for BAL-005-1

B. Requirements and Measures

R1. The Balancing Authority shall use a design scan rate of no more than six seconds in acquiring data necessary to calculate Reporting ACE. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M1. Each Balancing Authority will have dated documentation demonstrating that the data necessary to calculate Reporting ACE was designed to be scanned at a rate of no more than six seconds. Acceptable evidence may include historical data, dated archive files; or data from other databases, spreadsheets, or displays that demonstrate compliance.

R2. A Balancing Authority that is unable to calculate Reporting ACE for more than 30-consecutive minutes shall notify its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M2. Each Balancing Authority will have dated records to show when it was unable to calculate Reporting ACE for more than 30 consecutive minutes and that it notified its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE. Such evidence may include, but is not limited to, dated voice recordings, operating logs, or other communication documentation.

R3. Each Balancing Authority shall use frequency metering equipment for the calculation of Reporting ACE: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

3.1. that is available a minimum of 99.95% for each calendar year; and,

3.2. with a minimum accuracy of 0.001 Hz.

M3. The Balancing Authority shall have evidence such as dated documents or other evidence in hard copy or electronic format showing the frequency metering equipment used for the calculation of Reporting ACE had a minimum availability of 99.95% for each calendar year and had a minimum accuracy of 0.001 Hz to demonstrate compliance with Requirement R3.

R4. The Balancing Authority shall make available to the operator information associated with Reporting ACE including, but not limited to, quality flags indicating missing or invalid data. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. Each Balancing Authority Area shall have evidence such as a graphical display or dated alarm log that provides indication of data validity for the real-time Reporting ACE based on both the calculated result and all of the associated inputs therein.

R5. Each Balancing Authority's system used to calculate Reporting ACE shall be available a minimum of 99.5% of each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M5. Each Balancing Authority will have dated documentation demonstrating that the system necessary to calculate Reporting ACE has a minimum availability of 99.5% for each calendar year. Acceptable evidence may include historical data, dated archive files; or data from other databases, spreadsheets, or displays that demonstrate compliance.

R6. Each Balancing Authority that is within a multiple Balancing Authority Interconnection shall implement an Operating Process to identify and mitigate errors affecting the accuracy of scan rate data used in the calculation of Reporting ACE for each Balancing Authority Area. *[Violation Risk Factor: Medium] [Time Horizon: Same-day Operations]*

M6. Each Balancing Authority shall have a current Operating Process meeting the provisions of Requirement R6 and evidence to show that the process was implemented, such as dated communications or incorporation in System Operator task verification.

R7. Each Balancing Authority shall ensure that each Tie-Line, Pseudo-Tie, and Dynamic Schedule with an Adjacent Balancing Authority is equipped with: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **7.1.** a common source to provide information to both Balancing Authorities for the scan rate values used in the calculation of Reporting ACE; and,
- **7.2.** a time synchronized common source to determine hourly megawatt-hour values agreed-upon to aid in the identification and mitigation of errors.

M7. The Balancing Authority shall have dated evidence such as voice recordings or transcripts, operator logs, electronic communications, or other equivalent evidence that will be used to demonstrate a common source for the components used in the calculation of Reporting ACE with its Adjacent Balancing Authority.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" 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 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 applicable entity shall keep data or evidence to show compliance for the current year, plus three previous calendar years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" 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

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Real-time Operations	Medium	N/A	N/A	N/A	Balancing Authority was using a design scan rate of greater than six seconds to acquire the data necessary to calculate Reporting ACE.
R2.	Real-time Operations	Medium	The Balancing Authority failed to notify its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 50 minutes from the beginning of the	The Balancing Authority failed to notify its Reliability Coordinator within 50 minutes of the beginning of an inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 55 minutes from the beginning of an	The Balancing Authority failed to notify its Reliability Coordinator within 55 minutes of the beginning of an inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 60 minutes from the beginning of an	The Balancing Authority failed to notify its Reliability Coordinator within 60 minutes of the beginning of an inability to calculate Reporting ACE.

			inability to calculate Reporting ACE.	inability to calculate Reporting ACE.	inability to calculate Reporting ACE.	
R3.	Real-time Operations	Medium	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.95% of the calendar year but was available greater than or equal to 99.94 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.94% of the calendar year but was available greater than or equal to 99.93 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.93% of the calendar year but was available greater than or equal to 99.92 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.92% of the calendar year Or The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE failed to have a minimum accuracy of 0.001 Hz.
R4.	Real-time Operations	Medium	N/A	N/A	N/A	The Balancing Authority failed to make available information indicating missing or invalid data associated with

						Reporting ACE to its operators.
R5.	Operations Assessment	Medium	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.5% of the calendar year but was available greater than or equal to 99.4 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.4% of the calendar year but was available greater than or equal to 99.3 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.3% of the calendar year but was available greater than or equal to 99.2 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.2% of the calendar year.
R6.	Same-day Operations	Medium	N/A	N/A	N/A	The Balancing Authority failed to implement an Operating Process to identify and mitigate errors affecting the scan-rate accuracy of data used in the calculation of Reporting ACE.
R7.	Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority failed to use a common source for Tie-Lines, Pseudo-ties and Dynamic

						Schedules with its Adjacent Balancing Authorities **Or** **The Balancing Authority failed to use a time synchronized common source for hourly megawatt hour values that are agreed-upon to aid in the identification and mitigation of errors.**

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition

0.2b	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
0.2b	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02) effective January 21, 2014.	
1	February 11, 2016	Adopted by NERC Board of Trustees	Complete re-write of standard
1	September 20. 2017	FERC Order No. 836 approved BAL-005-1.	
1	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

Supplemental Material

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 R1: Real-time operation of a Balancing Authority requires real-time information. A sufficient scan rate is key to an Operator's trust in real-time information. Without a sufficient scan rate, an operator may question the accuracy of data during events, which would degrade the operator's ability to maintain reliability.

Rationale for Requirement R2: The RC is responsible for coordinating the reliability of bulk electric systems for member BA's. When a BA is unable to calculate its ACE for an extended period of time, this information must be communicated to the RC within 15 minutes thereafter so that the RC has sufficient knowledge of system conditions to assess any unintended reliability consequences that may occur on the wide area.

Rationale for Requirement R3: Frequency is the basic measurement for interconnection health, and a critical component for calculating Reporting ACE. Without sufficient available frequency data the BA operator will lack situational awareness and will be unable to make correct decisions when maintaining reliability.

Rationale for Requirement R4: System operators utilize Reporting ACE as a primary metric to determine operating actions or instructions. When data inputs into the ACE calculation are incorrect, the operator should be made aware through visual display. When an operator questions the validity of data, actions are delayed and the probability of adverse events occurring can increase.

Rationale for Requirement R5: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Since Reporting ACE is a measure of the BA's reliability performance for BAL-001, and BAL-002, it is critical that Reporting ACE be sufficiently available to assure reliability.

Rationale for Requirement R6: Reporting ACE is a measure of the BA's reliability performance for BAL-001, and BAL-002. Without a process to address persistent errors in the ACE calculation, the operator can lose trust in the validity of Reporting ACE resulting in delayed or incorrect decisions regarding the reliability of the bulk electric system.

Rationale for Requirement R7: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Common source data is critical to calculating Reporting ACE that is consistent between Balancing Authorities. When data sources are not common, confusion can be created between BAs resulting in delayed or incorrect operator action.

~~Supplemental Material~~

~~The intent of Requirement R7 Part 7.1 is to provide accuracy in the measurement and calculations used in Reporting ACE. It specifies the need for common metering points for instantaneous values for the tie-line megawatt flow values between Balancing Authority Areas. Common data source requirements also apply to instantaneous values for pseudo-ties and dynamic schedules, and can extend to more than two Balancing Authorities that participate in allocating shares of a generation resource in supplementary regulation, for example.~~

~~The intent of Requirement R7 Part 7.2 is to enable accuracy in the measurements and calculations used in Reporting ACE. It specifies the need for common metering points for hourly accumulated values for the time synchronized tie line MWh values agreed-upon between Balancing Authority Areas. These time synchronized agreed-upon values are necessary for use in the Operating Process required in R6 to identify and mitigate errors in the scan-rate values used in Reporting ACE.~~

A. Introduction

1. **Title:** Loss of Control Center Functionality
2. **Number:** EOP-008-2
3. **Purpose:** Ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Reliability Coordinator
     - **4.1.2.** Transmission Operator
     - **4.1.3.** Balancing Authority
5. **Effective Date:** See the Implementation Plan for EOP-008-2.
6. **Standard-Only Definition:** None

B. Requirements and Measures

R1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a current Operating Plan describing the manner in which it continues to meet its functional obligations with regard to the reliable operations of the BES in the event that its primary control center functionality is lost. This Operating Plan for backup functionality shall include: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

- **1.1.** The location and method of implementation for providing backup functionality.
- **1.2.** A summary description of the elements required to support the backup functionality. These elements shall include:
  - **1.2.1.** Tools and applications to ensure that System Operators have situational awareness of the BES.
  - **1.2.2.** Data exchange capabilities.
  - **1.2.3.** Interpersonal Communications.
  - **1.2.4.** Power source(s).
  - **1.2.5.** Physical and cyber security.
- **1.3.** An Operating Process for keeping the backup functionality consistent with the primary control center.
- **1.4.** Operating Procedures, including decision authority, for use in determining when to implement the Operating Plan for backup functionality.
- **1.5.** A transition period between the loss of primary control center functionality and the time to fully implement the backup functionality that is less than or equal to two hours.

1.6. An Operating Process describing the actions to be taken during the transition period between the loss of primary control center functionality and the time to fully implement backup functionality elements identified in Requirement R1, Part 1.2. The Operating Process shall include:

1.6.1. A list of all entities to notify when there is a change in operating locations.

1.6.2. Actions to manage the risk to the BES during the transition from primary to backup functionality, as well as during outages of the primary or backup functionality.

1.6.3. Identification of the roles for personnel involved during the initiation and implementation of the Operating Plan for backup functionality.

M1. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a dated, current, and in effect Operating Plan for backup functionality in accordance with Requirement R1, in electronic or hardcopy format.

R2. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a copy of its current Operating Plan for backup functionality available at its primary control center and at the location providing backup functionality. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*

M2. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a dated, current, and in effect copy of its Operating Plan for backup functionality in accordance with Requirement R2, in electronic or hardcopy format, available at its primary control center and at the location providing backup functionality.

R3. Each Reliability Coordinator shall have a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards are applicable to the primary control center functionality. To avoid requiring a tertiary facility, a backup facility is not required during: *[Violation Risk Factor = High] [Time Horizon = Operations Planning]*

- Planned outages of the primary or backup facilities of two weeks or less
- Unplanned outages of the primary or backup facilities

M3. Each Reliability Coordinator shall provide dated evidence that it has a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality in accordance with Requirement R3.

R4. Each Balancing Authority and Transmission Operator shall have backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality

location) that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's primary control center functionality. To avoid requiring tertiary functionality, backup functionality is not required during: *[Violation Risk Factor = High] [Time Horizon = Operations Planning]*

- Planned outages of the primary or backup functionality of two weeks or less
- Unplanned outages of the primary or backup functionality

M4. Each Balancing Authority and Transmission Operator shall provide dated evidence that its backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's or Transmission Operator's primary control center functionality in accordance with Requirement R4.

R5. Each Reliability Coordinator, Balancing Authority, and Transmission Operator, shall annually review and approve its Operating Plan for backup functionality. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

5.1. An update and approval of the Operating Plan for backup functionality shall take place within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1.

M5. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have evidence that its dated, current, and in effect Operating Plan for backup functionality, in electronic or hardcopy format, has been reviewed and approved annually and that it has been updated within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1 in accordance with Requirement R5.

R6. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have primary and backup functionality that do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M6. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have dated evidence that its primary and backup functionality do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards in accordance with Requirement R6.

R7. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct and document results of an annual test of its Operating Plan that demonstrates: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

7.1. The transition time between the simulated loss of primary control center functionality and the time to fully implement the backup functionality.

7.2. The backup functionality for a minimum of two continuous hours.

M7. Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall provide evidence such as dated records, that it has completed and documented its annual test of its Operating Plan for backup functionality, in accordance with Requirement R7.

R8. Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of its primary or backup functionality and that anticipates that the loss of primary or backup functionality will last for more than six calendar months shall provide a plan to its Regional Entity within six calendar months of the date when the functionality is lost, showing how it will re-establish primary or backup functionality. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

M8. Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of their primary or backup functionality and that anticipates that the loss of primary or backup functionality will last for more than six calendar months shall provide evidence that a plan has been submitted to its Regional Entity within six calendar months of the date when the functionality is lost showing how it will re-establish primary or backup functionality 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.

- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain its dated, current, in effect Operating Plan for backup functionality plus all issuances of the Operating Plan for backup functionality since its last compliance audit in accordance with Measurement M1.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain a dated, current, in effect copy of its Operating Plan for backup functionality, with evidence of its last issue, available at its primary control center and at the location providing backup functionality, for the current year, in accordance with Measurement M2.
- Each Reliability Coordinator shall retain dated evidence for the time period since its last compliance audit, that it has demonstrated that it has a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) in accordance with Requirement R3 that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality in accordance with Measurement M3.
- Each Balancing Authority and Transmission Operator shall retain dated evidence for the time period since its last compliance audit, that it has demonstrated that it's backup functionality (provided either through a facility or contracted services staffed by applicable certified operators

when control has been transferred to the backup functionality location) in accordance with Requirement R4 includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's primary control center functionality in accordance with Measurement M4.

- Each Reliability Coordinator, Balancing Authority, and Transmission Operator, shall retain evidence for the time period since its last compliance audit, that its dated, current, in effect Operating Plan for backup functionality, has been reviewed and approved annually and that it has been updated within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1 in accordance with Measurement M5.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain dated evidence for the current year and for any Operating Plan for backup functionality in effect since its last compliance audit, that its primary and backup functionality do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards in accordance with Measurement M6.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall retain evidence for the current calendar year and the previous calendar years, such as dated records, that it has tested its Operating Plan for backup functionality, in accordance with Measurement M7.
- Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of their primary or backup functionality and that anticipates that the loss of primary or backup functionality would last for more than six calendar months shall retain evidence for the current in effect document and any such documents in effect since its last compliance audit that a plan has been submitted to its Regional Entity within six calendar months of the date when the functionality is lost showing how it will re-establish primary or backup functionality in accordance with Measurement M8.

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 had a current Operating Plan for backup functionality, but the plan was missing one of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6).	The responsible entity had a current Operating Plan for backup functionality, but the plan was missing two of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6).	The responsible entity had a current Operating Plan for backup functionality, but the plan was missing three of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6).	The responsible entity had a current Operating Plan for backup functionality, but the plan was missing four or more of the requirement's six parts (Requirement R1, Parts 1.1 through 1.6) OR The responsible entity did not have a current Operating Plan for backup functionality.
R2.	N/A	The responsible entity did not have a copy of its current Operating Plan for backup functionality available in at least one of its control locations.	N/A	The responsible entity did not have a copy of its current Operating Plan for backup functionality at any of its locations.
R3.	N/A	N/A	N/A	The Reliability Coordinator does not have a backup control center facility (provided through its own dedicated backup facility or at another entity's control

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality.
R4.	N/A	N/A	N/A	The responsible entity does not have backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				primary control center functionality.
R5.	The responsible entity did not update and approve its Operating Plan for backup functionality for more than 60 calendar days and less than or equal to 70 calendar days after a change to any part of the Operating Plan described in Requirement R1.	The responsible entity did not update and approve its Operating Plan for backup functionality for more than 70 calendar days and less than or equal to 80 calendar days after a change to any part of the Operating Plan described in Requirement R1.	The responsible entity did not update and approve its Operating Plan for backup functionality for more than 80 calendar days and less than or equal to 90 calendar days after a change to any part of the Operating Plan described in Requirement R1.	The responsible entity did not have evidence that its Operating Plan for backup functionality was annually reviewed and approved. OR, The responsible entity did not update and approve its Operating Plan for backup functionality for more than 90 calendar days after a change to any part of the Operating Plan described in Requirement R1.
R6.	N/A	N/A	N/A	The responsible entity has primary and backup functionality that do depend on each other for the control center functionality required to maintain compliance with Reliability Standards.
R7.	The responsible entity conducted an annual test of	The responsible entity conducted an annual test of	The responsible entity conducted an annual test of	The responsible entity did not conduct an annual test

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	its Operating Plan for backup functionality, but it did not document the results. OR, The responsible entity conducted an annual test of its Operating Plan for backup functionality, but the test was for less than two continuous hours but more than or equal to 1.5 continuous hours.	its Operating Plan for backup functionality, but the test was for less than 1.5 continuous hours but more than or equal to 1 continuous hour.	its Operating Plan for backup functionality, but the test did not assess the transition time between the simulated loss of its primary control center and the time to fully implement the backup functionality OR, The responsible entity conducted an annual test of its Operating Plan for backup functionality, but the test was for less than 1 continuous hour but more than or equal to 0.5 continuous hours.	of its Operating Plan for backup functionality. OR, The responsible entity conducted an annual test of its Operating Plan for backup functionality, but the test was for less than 0.5 continuous hours.
R8.	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months and provided a plan to its	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months provided a plan to its Regional Entity	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months provided a plan to its Regional Entity	The responsible entity experienced a loss of its primary or backup functionality and anticipated that the loss of primary or backup functionality would last for more than six calendar months, but did not submit a plan to its Regional

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Regional Entity showing how it will re-establish primary or backup functionality but the plan was submitted more than six calendar months but less than or equal to seven calendar months after the date when the functionality was lost.	showing how it will re-establish primary or backup functionality but the plan was submitted in more than seven calendar months but less than or equal to eight calendar months after the date when the functionality was lost.	showing how it will re-establish primary or backup functionality but the plan was submitted in more than eight calendar months but less than or equal to nine calendar months after the date when the functionality was lost.	Entity showing how it will re-establish primary or backup functionality for more than nine calendar months after the date when the functionality was lost.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	2009 - 2010	Project 2006-04: Revisions	Major re-write to accommodate changes noted in project file
1	August 5, 2010	Project 2006-04: Adopted by the Board	
1	April 21, 2011	Project 2006-04: FERC Order issued approving EOP-008-1 (approval effective June 27, 2011)	
1	July 1, 2013	Project 2006-04: Updated VRFs and VSLs based on June 24, 2013 approval	
2	July 9, 2017	Adopted by the NERC Board of Trustees	Revised
2	January 18, 2018	FERC order issued approving EOP-008-2. Docket No. RM17-12-000.	
2	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

Supplemental Material

Rationale

Rationale for Requirement R1: The phrase "data exchange capabilities" is replacing “data communications in Requirement R1, Part 1.2.2 for the following reasons:

COM-001-1 (no longer enforceable) covered telecommunications, which could be viewed as covering both voice and data. COM-001-2.1 (currently enforceable) focuses on "Interpersonal Communication" and does not address data.

The topic of data exchange has historically been covered in the IRO / TOP Standards. Most recently the revisions to the standards that came out of Project 2014-03 Revisions to TOP and IRO Standards use the phrase "data exchange capabilities." The rationale included in the IRO-002-4 standard discusses the need to retain the topic of data exchange, as it is not addressed in the COM standards.

A. Introduction

1. **Title:** **Nuclear Plant Interface Coordination**

2. **Number:** **NUC-001-3**

3. **Purpose:** This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Nuclear Plant Generator Operators.

   4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

   4.2.1 Transmission Operators.

   4.2.2 Transmission Owners.

   4.2.3 Transmission Planners.

   4.2.4 Transmission Service Providers.

   4.2.5 Balancing Authorities.

   4.2.6 Reliability Coordinators.

   4.2.7 Planning Coordinators.

   4.2.8 Distribution Providers.

   4.2.9 Load-Serving Entities.

   4.2.10 Generator Owners.

   4.2.11 Generator Operators.

5. **Background:** Project 2012-13 Nuclear Power Interface Coordination seeks to implement the changes that were proposed by the NUC FYRT. The NUC FYRT was appointed by the Standards Committee Executive Committee on April 22, 2013. The NUC FYRT reviewed the NUC-001-2.1 standard to identify opportunities for consolidation and additional improvements. The NUC FYRT posted its recommendation to revise NUC-001-2.1 for industry comment on July 27, 2013. The NUC FYRT considered comments and submitted its final recommendation to revise NUC-001-2.1, along with a Standards Authorization Request (SAR) to the Standards Committee on October 17, 2013. The Standards Committee accepted the

recommendation of the FYRT and appointed the team as the Standard Drafting Team (SDT) to implement the recommendation.

6. **Effective Dates:** First day of the first calendar quarter that is twelve months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is twelve months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities.

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the currently effective Agreement(s) which document how the Nuclear Plant Generator Operator and the applicable Transmission Entities address and implement the NPIRs available for inspection upon request of the Compliance Enforcement Authority.

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator.: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement

[1] Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

Authority shall refer to the Agreements developed in accordance with this standard for specific requirements.

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall *[Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-time Operations]*

4.1. Incorporate the NPIRs into their operating analyses of the electric system.
4.2. Operate the electric system to meet the NPIRs.

4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:

- The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)
- The electric system was operated to meet the NPIRs. (Requirement 4.2)
- The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs

R5. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall operate the nuclear plant to meet the NPIRs. *[Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-time Operations]*

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the nuclear power plant is being operated consistent with the NPIRs.

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs.

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design (e.g., protective relay setpoints),

configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the Transmission Entities to meet the NPIRs.

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M8. The Transmission Entities shall each provide evidence that the entities informed the Nuclear Plant Generator Operator of changes to electric system design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs.

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include the following elements in aggregate within the Agreement(s) identified in R2.

- Where multiple Agreements with a single Transmission Entity are put into effect, the R9 elements must be addressed in aggregate within the Agreements; however, each Agreement does not have to contain each element. The Nuclear Plant Generator Operator and the Transmission Entity are responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements.
- Where Agreements with multiple Transmission Entities are required, the Nuclear Plant Generator Operator is responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements with the Transmission Entities. The Agreements with each Transmission Entity do not have to contain each element; however, the Agreements with the multiple Transmission Entities, in the aggregate, must address all R9 elements. For each Agreement(s), the Nuclear Plant Generator Operator and the Transmission Entity are responsible to ensure the Agreement(s) contain(s) the elements of R9 applicable to that Transmission Entity. : *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

9.1. Retired. *[Note: Part 9.1 was retired under the Paragraph 81 project. The NUC SDT proposes to leave this Part blank to avoid renumbering Requirement parts that would impact existing agreements throughout the industry.]*

9.2. Technical requirements and analysis:

9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the Agreement.

9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

9.3. Operations and maintenance coordination

9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.

9.3.6. Coordination of physical and cyber security protection at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

9.3.7. Coordination of the NPIRs with transmission system Remedial Action Schemes and any programs that reduce or shed load based on underfrequency or undervoltage.

9.4. Communications and training Administrative elements:

9.4.1. Provisions for communications affecting the NPIRs between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of applicable unique terms.

9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

9.4.5. Provisions for personnel training, as related to NPIRs.

M9. The Nuclear Plant Generator Operator shall have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. Each Transmission Entity shall have a copy of the Agreement(s) addressing the elements in Requirement 9 for which it is responsible available for inspection upon request of the Compliance Enforcement Authority.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.3. Data Retention

The 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:

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force Agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.

- For Measures 4, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

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

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		**Medium**	The Nuclear Plant Generator Operator provided the NPIRs to the applicable entities but did not verify receipt.	The Nuclear Plant Generator Operator did not provide the proposed NPIR to one of the applicable entities unless there was only one entity.	The Nuclear Plant Generator Operator did not provide the proposed NPIRs to two of the applicable entities unless there were only two entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIRs to more than two of applicable entities. OR For a particular nuclear power plant, if the number of possible applicable transmission entities is equal to the number of applicable transmission entities not provided NPIRs
R2		**Medium**	N/A	N/A	N/A	The Nuclear Plant Generator Operator or the applicable Transmission Entity does not have in effect one or more agreements that include mutually agreed to NPIRs and document the implementation of the NPIRs.
R3		**Medium**	N/A	The responsible entity incorporated the NPIRs into its planning analyses but did not communicate	N/A	The responsible entity did not incorporate the NPIRs into its planning analyses of the electric system.

				the results to the Nuclear Plant Generator Operator.		
R4		**High**	N/A	The responsible entity did not comply with Requirement R4, Part 4.3.	The responsible entity did not comply with Requirement R4, Part R4.1.	The responsible entity did not comply with Requirement R4, Part R4.2.
R5		**High**	N/A	N/A	N/A	The Nuclear Plant Generator Operator failed to operate per the NPIRs developed in accordance with this standard.
R6		**Medium**	N/A	The Nuclear Plant Generator Operator or Transmission Entity failed to provide outage or maintenance schedules to the appropriate parties as described in the agreement or on a time period consistent with the agreements.	The Nuclear Plant Generator Operator or Transmission Entity failed to coordinate one or more outages or maintenance activities in accordance the requirements of the agreements.	N/A
R7		**High**	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of proposed changes to nuclear plant design (e.g. protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs.	N/A	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of actual changes to nuclear plant design (e.g. protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of actual changes to nuclear plant design (e.g., protective relay setpoints), configuration, operations, limits or capabilities that directly impact the ability of the electric system to meet the NPIRs.
R8		**High**	The applicable Transmission Entities did not inform the Nuclear	N/A	The applicable Transmission Entities did not inform the Nuclear	The applicable Transmission Entities did not inform the Nuclear

			Plant Generator Operator of proposed changes to transmission system design, configuration (e.g. protective relay setpoints), operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs.		Plant Generator Operator of actual changes to transmission system design (e.g. protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs.	Plant Generator Operator of actual changes to transmission system design (e.g. protective relay setpoints), configuration, operations, limits, or capabilities that directly impacts the ability of the electric system to meet the NPIRs.
R9		**Medium**		The Agreement(s) identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entity failed to include up to 20% of the combined sub-components in Requirement R9 Parts 9.2, 9.3 and 9.4 applicable to that entity.	The Agreement(s) identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entity failed to include greater than 20%, but less than 40% of the combined sub-components in Requirement R9 Parts 9.2, 9.3 and 9.4 applicable to the entity.	The Agreement(s) identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entity failed to include 40% or more of the combined sub-components in Requirement R9 Parts 9.2, 9.3 and 9.4 applicable to the entity.

D. Regional Variances

The design basis for Canadian (CANDU) nuclear power plants (NPPs) does not result in the same licensing requirements as U.S. NPPs. Nuclear Regulatory Commission (NRC) design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. There are no equivalent Canadian Regulatory requirements for electrical power from the electric network to be provided to permit safe shutdown. Therefore the definition of Nuclear Plant Licensing Requirements (NPLR) for Canadian CANDU NPPs will be as follows:

Canadian Nuclear Plant Licensing Requirements (CNPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

E. Interpretations

None.

F. Associated Documents

None

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	August 5, 2009	Adopted by Board of Trustees	Revised. Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.
2	January 22, 2010	Approved by FERC on January 21, 2010. Added Effective Date	Update
2	February 7, 2013	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	

2	November 21, 2013	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
2.1	April 11, 2012	Errata approved by the Standards Committee; (Capitalized "Protection System" in accordance with Implementation Plan for Project 2007-17 approval of revised definition of "Protection System")	Errata associated with Project 2007-17
2.1	September 9, 2013	Informational filing submitted to reflect the revised definition of Protection System in accordance with the Implementation Plan for the revised term.	
3	March 2014	Modifications to implement the recommendations of the five-year review of NUC-001, which was accepted by the Standards Committee on October 17, 2013.	Revision
3	August 14, 2014	Adopted by the NERC Board of Trustees	
3	November 4, 2014	FERC letter order issued approving NUC-001-3	
3	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

~~**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 R5:**~~

~~The NUC FYRT recommended R5 be revised for consistency with R4 and to clarify that nuclear plants must be operated to meet the Nuclear Plant Interface Requirements.~~

~~**Rationale for R7 and R8:**~~

~~The NUC FYRT recommended deleting “Protection Systems” in Requirements R7 and R8 since it is a subset of the "nuclear plant design" and "electric system design" elements currently contained in R7 and R8 respectively; and adding a parenthetical clause (e.g. protective setpoints) to R7 following "nuclear plant design" and parenthetical clause (e.g. relay setpoints) to R8 following "electric system design."~~

~~Rationale for R9:~~

~~The NUC FYRT recommended that R9 be revised to clarify that all agreements do not have to discuss each of the elements in R9, but that the sum total of the agreements need to address the elements. In addition, for clarity in Part 9.4.1, the NUC FYRT recommended that "affecting the NPIRs" be inserted following "Provisions for communications" and "applicable unique" be inserted following ""definitions of."~~

~~Rationale for R9.3.7:~~

~~The term “Special Protection Systems” (SPS) was replaced with “Remedial Action Schemes” (RAS) in order to align with other current NERC standards development work in Project 2010-05.2: Special Protection Systems. Project 2010-05.2 has proposed to replace SPS with RAS throughout all of the NERC Standards in order to move to the use of a single term. RAS and SPS have the same definition in the NERC Glossary of Terms.~~

A. Introduction

1. **Title:** **Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance**

2. **Number: PRC-005-6**

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

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Transmission Owner

   4.1.2 Generator Owner

   4.1.3 Distribution Provider

   4.2. Facilities:

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

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

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

   4.2.4 Protection Systems installed as a Remedial Action Scheme (RAS) for BES reliability.

   4.2.5 Protection Systems and Sudden Pressure Relaying for generator Facilities that are part of the BES, except for generators identified through Inclusion I4 of the BES definition, including:

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

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

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

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

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

4.2.7 Automatic Reclosing[1], including:

4.2.7.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area or, if a member of a Reserve Sharing Group, the largest generating unit within the Reserve Sharing Group.[2]

4.2.7.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.7.1 when the substation is less than 10 circuit-miles from the generating plant substation.

4.2.7.3 Automatic Reclosing applied as an integral part of an RAS specified in Section 4.2.4.

5. **Effective Date:** See the Implementation Plan for this standard.

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

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Supervisory relay(s) or function(s) – relay(s) or function(s) that perform voltage and/or sync check functions that enable or disable operation of the reclosing relay
- Voltage sensing devices associated with the supervisory relay(s) or function(s)

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

[2] The largest BES generating unit within the Balancing Authority Area or the largest generating unit within the Reserve Sharing Group, as applicable, is subject to change. As a result of such a change, the Automatic Reclosing Components subject to the standard could change effective on the date of such change.

- Control circuitry associated with the reclosing relay or supervisory relay(s) or function(s)

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

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

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

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

Component Type –

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

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

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

B. Requirements and Measures

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

The PSMP shall:

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

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

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented PSMP in accordance with Requirement R1.

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

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

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

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

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the

time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-3, and Table 5. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” 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 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 Transmission Owner, Generator 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.

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

For Requirement R2, Requirement R3, and Requirement R4, in cases where the interval of the maintenance activity is longer than the audit cycle, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the most recent performance of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component. In cases where the interval of the maintenance activity is shorter than the audit cycle, documentation of all performances (in accordance with the tables) of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component since the previous scheduled audit date shall be retained.

For Requirement R5 the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of Unresolved Maintenance Issues identified by the entity since the last audit, including all that were resolved since the last audit.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

Table of Compliance Elements

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

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

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	For Components included within a performance-based maintenance program, the entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.
R5	The entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 5 but less than or equal to 10 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 10 but less than or equal to 15 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

D. Regional Variances

None.

E. Interpretations

None.

Supplemental Reference Documents

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

1. *Supplementary Reference and FAQ - PRC-005-6 Protection System Maintenance,* Protection System Maintenance and Testing Standard Drafting Team (July 2015)
2. *Considerations for Maintenance and Testing of Auto-reclosing Schemes*, NERC System Analysis and Modeling Subcommittee, and NERC System Protection and Control Subcommittee (November 2012)
3. *Sudden Pressure Relays and Other Devices that Respond to Non-Electrical Quantities – SPCS Input for Standard Development in Response to FERC Order No. 758,* NERC System Protection and Control Subcommittee (December 2013)
4. *Sudden Pressure Relays and Other Devices that Respond to Non-Electrical Quantities* – Supplemental Information to Support Project 2007-17.3: Protection System Maintenance and Testing (October 31, 2014)

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
1	February 7, 2006	Adopted by NERC Board of Trustees	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. Changed "Timeframe" to "Time Frame" in item D, 1.2.
1	March 16, 2007	PRC-005-1 Approved by FERC. Docket No. RM06-16-000	

Version	Date	Action	Change Tracking
1a	February 17, 2011	Adopted by NERC Board of Trustees	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers developed in Project 2009-17
1a	September 26, 2011	Approved by FERC. Docket No. RD11-5-000	
1b	November 5, 2009	Adopted by NERC Board of Trustees	Interpretation of R1, R1.1, and R1.2 developed by Project 2009-10
1b	February 3, 2012	FERC Order approving revised definition of "Protection System"	Per footnote 8 of FERC's order, the definition of "Protection System" supersedes interpretation "b" of PRC-005-1b upon the effective date of the modified definition (i.e., April 1, 2013) *See N. Amer. Elec. Reliability Corp.*, 138 FERC ¶ 61,095 (February 3, 2012).
1b	February 3, 2012	PRC-005-1b Approved by FERC. Docket No. RM10-5-000	
1.1b	May 9, 2012	Adopted by NERC Board of Trustees	Errata change developed by Project 2010-07, clarified inclusion of generator interconnection Facility in Generator Owner's responsibility
1.1b	September 19, 2013	PRC-005-1.1b Approved by FERC. Docket No. RM12-16-000	
2	November 7, 2012	Adopted by NERC Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0

Version	Date	Action	Change Tracking
2	October 17, 2013	Approved by NERC Standards Committee	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase “or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;” to the second sentence under the “Retirement of Existing Standards” section. (no change to standard version number)
2	December 19, 2013	PRC-005-2 Approved by FERC. Docket No. RM13-7-000	
2	March 7, 2014	Adopted by NERC Board of Trustees	Modified R1 VSL in response to FERC directive (no change to standard version number)
2(i)	November 13, 2014	Adopted by NERC Board of Trustees	Applicability section revised by Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources
2(i)	May 29, 2015	PRC-005-2(i) Approved by FERC. Docket No. RD15-3-000	
2(ii)	November 13, 2014	Adopted by NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No. 758 to include Automatic Reclosing in maintenance programs

Version	Date	Action	Change Tracking
3	February 12, 2014	Approved by NERC Standards Committee	Errata Change: The Standards Committee approved errata changes to correct capitalization of certain defined terms within the definitions of “Unresolved Maintenance Issue” and “Protection System Maintenance Program”. The changes will be reflected in the definitions section of PRC-005-3 for “Unresolved Maintenance Issue” and in the NERC Glossary of Terms for “Protection System Maintenance Program". (no change to standard version number)
3	March 7, 2014	Adopted by NERC Board of Trustees	Modified R1 VSL in response to FERC directive (no change to standard version number)
3	January 22, 2015	PRC-005-3 Approved by FERC. Docket No. RM14-8-000	
3(i)	November 13, 2014	Adopted by NERC Board of Trustees	Applicability section revised by Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources
3(i)	May 29, 2015	PRC-005-3(i) Approved by FERC. Docket No. RD15-3-000	
3(ii)	November 13, 2014	Adopted by NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS
4	November 13, 2014	Adopted by NERC Board of Trustees	Added Sudden Pressure Relaying in response to FERC Order No. 758
4	Sept 17, 2015	PRC-005-4 Approved by FERC. Docket No. RM15-9-000	

Version	Date	Action	Change Tracking
5	May 7, 2015	Adopted by NERC Board of Trustees	Applicability section revised by Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources.
6	November 5, 2015	Adopted by NERC Board of Trustees	Revised to add supervisory relays, the voltage sensing devices, and the associated control circuitry to Automatic Reclosing in accordance with the directives in FERC Order 803.
6	December 18, 2015	FERC Letter Order approving PRC-005-6. Docket No. RD16-2-000.	
6	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 4-1

Maintenance Activities and Intervals for Automatic Reclosing Components

Component Type – Reclosing and Supervisory Relay

Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval.

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any unmonitored reclosing relay or supervisory relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor reclosing or supervisory relays: • Test and, if necessary calibrate For microprocessor reclosing or supervisory relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing. For microprocessor supervisory relays: • Verify acceptable measurement of power system input values.
• Monitored microprocessor reclosing relay or supervisory relay with the following: Internal self-diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2). For supervisory relay: • Voltage waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics.	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing. For supervisory relays: • Verify acceptable measurement of power system input values.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing and Supervisory Relay Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Monitored microprocessor reclosing relay or supervisory relay with preceding row attributes and the following: • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2). For supervisory relay: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that are NOT an Integral Part of an RAS Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an RAS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an RAS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that ARE an Integral Part of an RAS Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an RAS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an RAS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the RAS.
Control circuitry associated with Automatic Reclosing that is an integral part of an RAS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

Table 4-3 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Voltage Sensing Devices Associated with Supervisory Relays Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-3, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that voltage signal values are provided to the supervisory relays.
Voltage sensing devices that are connected to microprocessor supervisory relays with ac measurements that are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure. (See Table 2)	No periodic maintenance specified	None.

Table 5 Maintenance Activities and Intervals for Sudden Pressure Relaying Note: In cases where Components of Sudden Pressure Relaying are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any fault pressure relay.	6 Calendar Years	Verify the pressure or flow sensing mechanism is operable.
Electromechanical lockout devices which are directly in a trip path from the fault pressure relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with Sudden Pressure Relaying.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with Sudden Pressure Relaying whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

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

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

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

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

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

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

~~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 revisions to Automatic Reclosing:~~

~~To address directives from FERC Order No. 803 addressing Automatic Reclosing, the definition for Automatic Reclosing was revised to add supervisory relays, the associated voltage sensing devices, and the associated control circuitry.~~

~~Rationale for revisions to Component Type:~~

~~With the revision of the definition of Automatic Reclosing, there are four specific elements of this definition, rather than two as stated in the prior version.~~

A. Introduction

1. Title: **Automatic Underfrequency Load Shedding**

2. Number: PRC-006-3

3. Purpose: To establish design and documentation requirements for automatic underfrequency load shedding (UFLS) programs to arrest declining frequency, assist recovery of frequency following underfrequency events and provide last resort system preservation measures.

4. Applicability:

4.1. Planning Coordinators

4.2. UFLS entities shall mean all entities that are responsible for the ownership, operation, or control of UFLS equipment as required by the UFLS program established by the Planning Coordinators. Such entities may include one or more of the following:

4.2.1 Transmission Owners

4.2.2 Distribution Providers

4.3. Transmission Owners that own Elements identified in the UFLS program established by the Planning Coordinators.

5. Effective Date:

This standard is effective on the first day of the first calendar quarter six months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

6. Background:

PRC-006-2 was developed under Project 2008-02: Underfrequency Load Shedding (UFLS). The drafting team revised PRC-006-1 for the purpose of addressing the directive issued in FERC Order No. 763. *Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards*, 139 FERC ¶ 61,098 (2012).

B. Requirements and Measures

R1. Each Planning Coordinator shall develop and document criteria, including consideration of historical events and system studies, to select portions of the Bulk Electric System (BES), including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas that may form islands. *[VRF: Medium][Time Horizon: Long-term Planning]*

M1. Each Planning Coordinator shall have evidence such as reports, or other documentation of its criteria to select portions of the Bulk Electric System that may form islands including how system studies and historical events were considered to develop the criteria per Requirement R1.

R2. Each Planning Coordinator shall identify one or more islands to serve as a basis for designing its UFLS program including: *[VRF: Medium][Time Horizon: Long-term Planning]*

2.1. Those islands selected by applying the criteria in Requirement R1, and

2.2. Any portions of the BES designed to detach from the Interconnection (planned islands) as a result of the operation of a relay scheme or Special Protection System, and

2.3. A single island that includes all portions of the BES in either the Regional Entity area or the Interconnection in which the Planning Coordinator's area resides. If a Planning Coordinator's area resides in multiple Regional Entity areas, each of those Regional Entity areas shall be identified as an island. Planning Coordinators may adjust island boundaries to differ from Regional Entity area boundaries by mutual consent where necessary for the sole purpose of producing contiguous regional islands more suitable for simulation.

M2. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, or other documentation supporting its identification of an island(s) as a basis for designing a UFLS program that meet the criteria in Requirement R2, Parts 2.1 through 2.3.

R3. Each Planning Coordinator shall develop a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from an imbalance scenario, where an imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s). *[VRF: High][Time Horizon: Long-term Planning]*

3.1. Frequency shall remain above the Underfrequency Performance Characteristic curve in PRC-006-3 - Attachment 1, either for 60 seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

3.2. Frequency shall remain below the Overfrequency Performance Characteristic curve in PRC-006-3 - Attachment 1, either for 60 seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

3.3. Volts per Hz (V/Hz) shall not exceed 1.18 per unit for longer than two seconds cumulatively per simulated event, and shall not exceed 1.10 per unit for longer than 45 seconds cumulatively per simulated event at each generator bus and generator step-up transformer high-side bus associated with each of the following:

- Individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES
- Generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES
- Facilities consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA gross nameplate rating.

M3. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its UFLS program, including the notification of the UFLS entities of implementation schedule, that meet the criteria in Requirement R3, Parts 3.1 through 3.3.

R4. Each Planning Coordinator shall conduct and document a UFLS design assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2. The simulation shall model each of the following: *[VRF: High][Time Horizon: Long-term Planning]*

4.1. Underfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-3 - Attachment 1.

4.2. Underfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-3 - Attachment 1.

4.3. Underfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA (gross nameplate rating) that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-3 - Attachment 1.

4.4. Overfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-3 — Attachment 1.

4.5. Overfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-3 — Attachment 1.

4.6. Overfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA

(gross nameplate rating) that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-3 — Attachment 1.

4.7. Any automatic Load restoration that impacts frequency stabilization and operates within the duration of the simulations run for the assessment.

M4. Each Planning Coordinator shall have dated evidence such as reports, dynamic simulation models and results, or other dated documentation of its UFLS design assessment that demonstrates it meets Requirement R4, Parts 4.1 through 4.7.

R5. Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall coordinate its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island through one of the following: *[VRF: High][Time Horizon: Long-term Planning]*

- Develop a common UFLS program design and schedule for implementation per Requirement R3 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or
- Conduct a joint UFLS design assessment per Requirement R4 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or
- Conduct an independent UFLS design assessment per Requirement R4 for the identified island, and in the event the UFLS design assessment fails to meet Requirement R3, identify modifications to the UFLS program(s) to meet Requirement R3 and report these modifications as recommendations to the other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island and the ERO.

M5. Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall have dated evidence such as joint UFLS program design documents, reports describing a joint UFLS design assessment, letters that include recommendations, or other dated documentation demonstrating that it coordinated its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island per Requirement R5.

R6. Each Planning Coordinator shall maintain a UFLS database containing data necessary to model its UFLS program for use in event analyses and assessments of the UFLS program at least once each calendar year, with no more than 15 months between maintenance activities. *[VRF: Lower][Time Horizon: Long-term Planning]*

M6. Each Planning Coordinator shall have dated evidence such as a UFLS database, data requests, data input forms, or other dated documentation to show that it maintained a UFLS database for use in event analyses and assessments of the UFLS program per

Requirement R6 at least once each calendar year, with no more than 15 months between maintenance activities.

R7. Each Planning Coordinator shall provide its UFLS database containing data necessary to model its UFLS program to other Planning Coordinators within its Interconnection within 30 calendar days of a request. *[VRF: Lower][Time Horizon: Long-term Planning]*

M7. Each Planning Coordinator shall have dated evidence such as letters, memorandums, e-mails or other dated documentation that it provided their UFLS database to other Planning Coordinators within their Interconnection within 30 calendar days of a request per Requirement R7.

R8. Each UFLS entity shall provide data to its Planning Coordinator(s) according to the format and schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. *[VRF: Lower][Time Horizon: Long-term Planning]*

M8. Each UFLS Entity shall have dated evidence such as responses to data requests, spreadsheets, letters or other dated documentation that it provided data to its Planning Coordinator according to the format and schedule specified by the Planning Coordinator to support maintenance of the UFLS database per Requirement R8.

R9. Each UFLS entity shall provide automatic tripping of Load in accordance with the UFLS program design and schedule for implementation, including any Corrective Action Plan, as determined by its Planning Coordinator(s) in each Planning Coordinator area in which it owns assets. *[VRF: High][Time Horizon: Long-term Planning]*

M9. Each UFLS Entity shall have dated evidence such as spreadsheets summarizing feeder load armed with UFLS relays, spreadsheets with UFLS relay settings, or other dated documentation that it provided automatic tripping of load in accordance with the UFLS program design and schedule for implementation, including any Corrective Action Plan, per Requirement R9.

R10. Each Transmission Owner shall provide automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission. *[VRF: High][Time Horizon: Long-term Planning]*

M10. Each Transmission Owner shall have dated evidence such as relay settings, tripping logic or other dated documentation that it provided automatic switching of its existing capacitor banks, Transmission Lines, and reactors in order to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, per Requirement R10.

R11. Each Planning Coordinator, in whose area a BES islanding event results in system frequency excursions below the initializing set points of the UFLS program, shall

conduct and document an assessment of the event within one year of event actuation to evaluate: *[VRF: Medium][Time Horizon: Operations Assessment]*

11.1. The performance of the UFLS equipment,

11.2. The effectiveness of the UFLS program.

M11. Each Planning Coordinator shall have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it conducted an event assessment of the performance of the UFLS equipment and the effectiveness of the UFLS program per Requirement R11.

R12. Each Planning Coordinator, in whose islanding event assessment (per R11) UFLS program deficiencies are identified, shall conduct and document a UFLS design assessment to consider the identified deficiencies within two years of event actuation. *[VRF: Medium][Time Horizon: Operations Assessment]*

M12. Each Planning Coordinator shall have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it conducted a UFLS design assessment per Requirements R12 and R4 if UFLS program deficiencies are identified in R11.

R13. Each Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, shall coordinate its event assessment (in accordance with Requirement R11) with all other Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event through one of the following: *[VRF: Medium][Time Horizon: Operations Assessment]*

- Conduct a joint event assessment per Requirement R11 among the Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or
- Conduct an independent event assessment per Requirement R11 that reaches conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or
- Conduct an independent event assessment per Requirement R11 and where the assessment fails to reach conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, identify differences in the assessments that likely resulted in the differences in the conclusions and recommendations and report these differences to the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event and the ERO.

M13. Each Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same

islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, shall have dated evidence such as a joint assessment report, independent assessment reports and letters describing likely reasons for differences in conclusions and recommendations, or other dated documentation demonstrating it coordinated its event assessment (per Requirement R11) with all other Planning Coordinator(s) whose areas or portions of whose areas were also included in the same islanding event per Requirement R13.

R14. Each Planning Coordinator shall respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the following *[VRF: Lower][Time Horizon: Long-term Planning]*:

14.1. UFLS program, including a schedule for implementation

14.2. UFLS design assessment

14.3. Format and schedule of UFLS data submittal

M14. Each Planning Coordinator shall have dated evidence of responses, such as e-mails and letters, to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program per Requirement R14.

R15. Each Planning Coordinator that conducts a UFLS design assessment under Requirement R4, R5, or R12 and determines that the UFLS program does not meet the performance characteristics in Requirement R3, shall develop a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area. *[VRF: High][Time Horizon: Long-term Planning]*

15.1. For UFLS design assessments performed under Requirement R4 or R5, the Corrective Action Plan shall be developed within the five-year time frame identified in Requirement R4.

15.2. For UFLS design assessments performed under Requirement R12, the Corrective Action Plan shall be developed within the two-year time frame identified in Requirement R12.

M15. Each Planning Coordinator that conducts a UFLS design assessment under Requirement R4, R5, or R12 and determines that the UFLS program does not meet the performance characteristics in Requirement R3, shall have a dated Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, that was developed within the time frame identified in Part 15.1 or 15.2.

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

Each Planning Coordinator and UFLS 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 Planning Coordinator shall retain the current evidence of Requirements R1, R2, R3, R4, R5, R12, R14, and R15, Measures M1, M2, M3, M4, M5, M12, M14, and M15 as well as any evidence necessary to show compliance since the last compliance audit.
- Each Planning Coordinator shall retain the current evidence of UFLS database update in accordance with Requirement R6, Measure M6, and evidence of the prior year's UFLS database update.
- Each Planning Coordinator shall retain evidence of any UFLS database transmittal to another Planning Coordinator since the last compliance audit in accordance with Requirement R7, Measure M7.
- Each UFLS entity shall retain evidence of UFLS data transmittal to the Planning Coordinator(s) since the last compliance audit in accordance with Requirement R8, Measure M8.
- Each UFLS entity shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R9, Measure M9, and evidence of adherence since the last compliance audit.
- Transmission Owner shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R10, Measure M10, and evidence of adherence since the last compliance audit.
- Each Planning Coordinator shall retain evidence of Requirements R11, and R13, and Measures M11, and M13 for 6 calendar years.

If a Planning Coordinator or UFLS entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the retention period specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas that may form islands. OR The Planning Coordinator developed and documented criteria but failed to include the consideration of system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events and system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.	The Planning Coordinator failed to develop and document criteria to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.
R2	N/A	The Planning Coordinator identified an island(s) to	The Planning Coordinator identified an island(s) to serve	The Planning Coordinator identified an island(s) to serve

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
		serve as a basis for designing its UFLS program but failed to include one (1) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	as a basis for designing its UFLS program but failed to include two (2) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	as a basis for designing its UFLS program but failed to include all of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3. OR The Planning Coordinator failed to identify any island(s) to serve as a basis for designing its UFLS program.
R3	N/A	The Planning Coordinator developed a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet one (1) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet two (2) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s).,but failed to meet all the performance characteristic in Requirement R3, Parts 3.1, 3.2, and 3.3 in simulations of underfrequency conditions. OR The Planning Coordinator failed to develop a UFLS program

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				including notification of and a schedule for implementation by UFLS entities within its area
R4	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include one (1) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include two (2) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include three (3) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 but simulation failed to include four (4) or more of the items as specified in Requirement R4, Parts 4.1 through 4.7. OR The Planning Coordinator failed to conduct and document a UFLS assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	N/A	N/A	N/A	The Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, failed to coordinate its UFLS program design through one of the manners described in Requirement R5.
R6	N/A	N/A	N/A	The Planning Coordinator failed to maintain a UFLS database for use in event analyses and assessments of the UFLS program at least once each calendar year, with no more than 15 months between maintenance activities.
R7	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 30 calendar days and up to and including 40 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 40 calendar days but less than and including 50 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 50 calendar days but less than and including 60 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 60 calendar days following the request. OR

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Planning Coordinator failed to provide its UFLS database to other Planning Coordinators.
R8	The UFLS entity provided data to its Planning Coordinator(s) less than or equal to 10 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 10 calendar days but less than or equal to 15 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR The UFLS entity provided data to its Planning Coordinator(s) but the data was not according to the format specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 15 calendar days but less than or equal to 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR The UFLS entity failed to provide data to its Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.
R9	The UFLS entity provided less than 100% but more than (and including) 95% of automatic tripping of Load in accordance with the UFLS	The UFLS entity provided less than 95% but more than (and including) 90% of automatic tripping of Load in accordance with the UFLS program design	The UFLS entity provided less than 90% but more than (and including) 85% of automatic tripping of Load in accordance with the UFLS program design	The UFLS entity provided less than 85% of automatic tripping of Load in accordance with the UFLS program design and schedule for implementation,

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	program design and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.	and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.	and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.	including any Corrective Action Plan, as determined by the Planning Coordinator(s) area in which it owns assets.
R10	The Transmission Owner provided less than 100% but more than (and including) 95% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 95% but more than (and including) 90% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 90% but more than (and including) 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.
R11	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program,

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than one year but less than or equal to 13 months of actuation.	the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 13 months but less than or equal to 14 months of actuation.	UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 14 months but less than or equal to 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate one (1) of the Parts as specified in Requirement R11, Parts11.1 or 11.2.	conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, failed to conduct and document an assessment of the event and evaluate the Parts as specified in Requirement R11, Parts 11.1 and 11.2. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate all of the Parts

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				as specified in Requirement R11, Parts 11.1 and 11.2.
R12	N/A	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS design assessment to consider the identified deficiencies greater than two years but less than or equal to 25 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS design assessment to consider the identified deficiencies greater than 25 months but less than or equal to 26 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS design assessment to consider the identified deficiencies greater than 26 months of event actuation. OR The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, failed to conduct and document a UFLS design assessment to consider the identified deficiencies.
R13	N/A	N/A	N/A	The Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				program, failed to coordinate its UFLS event assessment with all other Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event in one of the manners described in Requirement R13
R14	N/A	N/A	N/A	The Planning Coordinator failed to respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes were made or reasons why changes were not made to the items in Parts 14.1 through 14.3.
R15	N/A	The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement	The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement	The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3, and developed a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, but exceeded the permissible time frame for development by a period of up to 1 month.	R3, and developed a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, but exceeded the permissible time frame for development by a period greater than 1 month but not more than 2 months.	R3, but failed to develop a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area. OR The Planning Coordinator determined, through a UFLS design assessment performed under Requirement R4, R5, or R12, that the UFLS program did not meet the performance characteristics in Requirement R3, and developed a Corrective Action Plan and a schedule for implementation by the UFLS entities within its area, but exceeded the permissible time frame for development by a period greater than 2 months.

D. Regional Variances

D.A. Regional Variance for the Quebec Interconnection

The following Interconnection-wide variance shall be applicable in the Quebec Interconnection and replaces, in their entirety, Requirements R3 and R4 and the violation severity levels associated with Requirements R3 and R4.

Rationale for Requirement D.A.3:

There are two modifications for requirement D.A.3 :

1. 25% Generation Deficiency : Since the Quebec Interconnection has no potential viable BES Island in underfrequency conditions, the largest generation deficiency scenarios are limited to extreme contingencies not already covered by RAS.

Based on Hydro-Québec TransÉnergie Transmission Planning requirements, the stability of the network shall be maintained for extreme contingencies using a case representing internal transfers not expected to be exceeded 25% of the time.

The Hydro-Québec TransÉnergie defense plan to cover these extreme contingencies includes two RAS (RPTC- generation rejection and remote load shedding and TDST - a centralized UVLS) and the UFLS.

2. Frequency performance curve (attachment 1A) : Specific cases where a small generation deficiency using a peak case scenario with the minimum requirement of spinning reserve can lead to an acceptable frequency deviation in the Quebec Interconnection while stabilizing between the PRC-006-2 requirement (59.3 Hz) and the UFLS anti-stall threshold (59.0 Hz).

An increase of the anti-stall threshold to 59.3 Hz would correct this situation but would cause frequent load shedding of customers without any gain of system reliability. Therefore, it is preferable to lower the steady state frequency minimum value to 59.0 Hz.

The delay in the performance characteristics curve is harmonized between D.A.3 and R.3 to 60 seconds.

Rationale for Requirements D.A.3.3. and D.A.4:

The **Q**uebec Interconnection has its own definition of BES. In Quebec, the vast majority of BES generating plants/facilities are not directly connected to the BES. For simulations to take into account sufficient generating resources D.A.3.3 and D.A.4 need simply refer to BES generators, plants or facilities since these are listed in a Registry approved by Québec's Regulatory Body (Régie de l'Énergie).

D.A.3. Each Planning Coordinator shall develop a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, that

meets the following performance characteristics in simulations of underfrequency conditions resulting from each of these extreme events:

- Loss of the entire capability of a generating station.
- Loss of all transmission circuits emanating from a generating station, switching station, substation or dc terminal.
- Loss of all transmission circuits on a common right-of-way.
- Three-phase fault with failure of a circuit breaker to operate and correct operation of a breaker failure protection system and its associated breakers.
- Three-phase fault on a circuit breaker, with normal fault clearing.
- The operation or partial operation of a RAS for an event or condition for which it was not intended to operate.

[VRF: High][Time Horizon: Long-term Planning]

D.A.3.1. Frequency shall remain above the Underfrequency Performance Characteristic curve in PRC-006-3 - Attachment 1A, either for 60 seconds or until a steady-state condition between 59.0 Hz and 60.7 Hz is reached, and

D.A.3.2. Frequency shall remain below the Overfrequency Performance Characteristic curve in PRC-006-3 - Attachment 1A, either for 60 seconds or until a steady-state condition between 59.0 Hz and 60.7 Hz is reached, and

D.A.3.3. Volts per Hz (V/Hz) shall not exceed 1.18 per unit for longer than two seconds cumulatively per simulated event, and shall not exceed 1.10 per unit for longer than 45 seconds cumulatively per simulated event at each Quebec BES generator bus and associated generator step-up transformer high-side bus

M.D.A.3. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its UFLS program, including the notification of the UFLS entities of implementation schedule, that meet the criteria in Requirement D.A.3 Parts D.A.3.1 through D.A.3.3.

D.A.4. Each Planning Coordinator shall conduct and document a UFLS design assessment at least once every five years that determines through dynamic

simulation whether the UFLS program design meets the performance characteristics in Requirement D.A.3 for each island identified in Requirement R2. The simulation shall model each of the following; *[VRF: High][Time Horizon: Long-term Planning]*

D.A.4.1 Underfrequency trip settings of individual generating units that are part of Quebec BES plants/facilities that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-3 - Attachment 1A, and

D.A.4.2 Overfrequency trip settings of individual generating units that are part of Quebec BES plants/facilities that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-3 - Attachment 1A, and

D.A.4.3 Any automatic Load restoration that impacts frequency stabilization and operates within the duration of the simulations run for the assessment.

M.D.A.4. Each Planning Coordinator shall have dated evidence such as reports, dynamic simulation models and results, or other dated documentation of its UFLS design assessment that demonstrates it meets Requirement D.A.4 Parts D.A.4.1 through D.A.4.3.

D#	Lower VSL	Moderate VSL	High VSL	Severe VSL
DA3	N/A	The Planning Coordinator developed a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, but failed to meet one (1) of the performance characteristic in Parts D.A.3.1, D.A.3.2, or D.A.3.3 in simulations of underfrequency conditions	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area, but failed to meet two (2) of the performance characteristic in Parts D.A.3.1, D.A.3.2, or D.A.3.3 in simulations of underfrequency conditions	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area, but failed to meet all the performance characteristic in Parts D.A.3.1, D.A.3.2, and D.A.3.3 in simulations of underfrequency conditions OR The Planning Coordinator failed to develop a UFLS program including notification of and a schedule for implementation by UFLS entities within its area.
DA4	N/A	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement D.A.3 but the simulation failed to include one (1) of the items as	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement D.A.3 but the simulation failed to include two (2) of the items as	The Planning Coordinator conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement D.A.3 but the simulation failed to include all of the items as

D#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		specified in Parts D.A.4.1, D.A.4.2 or D.A.4.3.	specified in Parts D.A.4.1, D.A.4.2 or D.A.4.3.	specified in Parts D.A.4.1, D.A.4.2 and D.A.4.3. OR The Planning Coordinator failed to conduct and document a UFLS assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.A.3

D.B. Regional Variance for the Western Electricity Coordinating Council

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R1, R2, R3, R4, R5, R11, R12, and R13.

D.B.1. Each Planning Coordinator shall participate in a joint regional review with the other Planning Coordinators in the WECC Regional Entity area that develops and documents criteria, including consideration of historical events and system studies, to select portions of the Bulk Electric System (BES) that may form islands. *[VRF: Medium][Time Horizon: Long-term Planning]*

M.D.B.1. Each Planning Coordinator shall have evidence such as reports, or other documentation of its criteria, developed as part of the joint regional review with other Planning Coordinators in the WECC Regional Entity area to select portions of the Bulk Electric System that may form islands including how system studies and historical events were considered to develop the criteria per Requirement D.B.1.

D.B.2. Each Planning Coordinator shall identify one or more islands from the regional review (per D.B.1) to serve as a basis for designing a region-wide coordinated UFLS program including: *[VRF: Medium][Time Horizon: Long-term Planning]*

D.B.2.1. Those islands selected by applying the criteria in Requirement D.B.1, and

D.B.2.2. Any portions of the BES designed to detach from the Interconnection (planned islands) as a result of the operation of a relay scheme or Special Protection System.

M.D.B.2. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, or other documentation supporting its identification of an island(s), from the regional review (per D.B.1), as a basis for designing a region-wide coordinated UFLS program that meet the criteria in Requirement D.B.2 Parts D.B.2.1 and D.B.2.2.

D.B.3. Each Planning Coordinator shall adopt a UFLS program, coordinated across the WECC Regional Entity area, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from an imbalance scenario, where an imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s). *[VRF: High][Time Horizon: Long-term Planning]*

D.B.3.1. Frequency shall remain above the Underfrequency Performance Characteristic curve in PRC-006-3 - Attachment 1, either for 60 seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

D.B.3.2. Frequency shall remain below the Overfrequency Performance Characteristic curve in PRC-006-3 - Attachment 1, either for 60 seconds or until a steady-state condition between 59.3 Hz and 60.7 Hz is reached, and

D.B.3.3. Volts per Hz (V/Hz) shall not exceed 1.18 per unit for longer than two seconds cumulatively per simulated event, and shall not exceed 1.10 per unit for longer than 45 seconds cumulatively per simulated event at each generator bus and generator step-up transformer high-side bus associated with each of the following:

D.B.3.3.1. Individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES

D.B.3.3.2. Generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES

D.B.3.3.3. Facilities consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA gross nameplate rating.

M.D.B.3. Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its adoption of a UFLS program, coordinated across the WECC Regional Entity area, including the notification of the UFLS entities of implementation schedule, that meet the criteria in Requirement D.B.3 Parts D.B.3.1 through D.B.3.3.

D.B.4. Each Planning Coordinator shall participate in and document a coordinated UFLS design assessment with the other Planning Coordinators in the WECC Regional Entity area at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2. The simulation shall model each of the following: *[VRF: High][Time Horizon: Long-term Planning]*

D.B.4.1. Underfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-3 - Attachment 1.

D.B.4.2. Underfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-3 - Attachment 1.

D.B.4.3. Underfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation

above 75 MVA (gross nameplate rating) that trip above the Generator Underfrequency Trip Modeling curve in PRC-006-3 - Attachment 1.

D.B.4.4. Overfrequency trip settings of individual generating units greater than 20 MVA (gross nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-3 — Attachment 1.

D.B.4.5. Overfrequency trip settings of generating plants/facilities greater than 75 MVA (gross aggregate nameplate rating) directly connected to the BES that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-3 — Attachment 1.

D.B.4.6. Overfrequency trip settings of any facility consisting of one or more units connected to the BES at a common bus with total generation above 75 MVA (gross nameplate rating) that trip below the Generator Overfrequency Trip Modeling curve in PRC-006-3 — Attachment 1.

D.B.4.7. Any automatic Load restoration that impacts frequency stabilization and operates within the duration of the simulations run for the assessment.

M.D.B.4. Each Planning Coordinator shall have dated evidence such as reports, dynamic simulation models and results, or other dated documentation of its participation in a coordinated UFLS design assessment with the other Planning Coordinators in the WECC Regional Entity area that demonstrates it meets Requirement D.B.4 Parts D.B.4.1 through D.B.4.7.

D.B.11. Each Planning Coordinator, in whose area a BES islanding event results in system frequency excursions below the initializing set points of the UFLS program, shall participate in and document a coordinated event assessment with all affected Planning Coordinators to conduct and document an assessment of the event within one year of event actuation to evaluate: *[VRF: Medium][Time Horizon: Operations Assessment]*

D.B.11.1. The performance of the UFLS equipment,

D.B.11.2 The effectiveness of the UFLS program

M.D.B.11. Each Planning Coordinator shall have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it participated in a coordinated event assessment of the performance of the UFLS equipment and the effectiveness of the UFLS program per Requirement D.B.11.

D.B.12. Each Planning Coordinator, in whose islanding event assessment (per D.B.11) UFLS program deficiencies are identified, shall participate in and document a coordinated UFLS design assessment of the UFLS program with the other Planning Coordinators in the WECC Regional Entity area to consider the identified deficiencies within two years of event actuation. *[VRF: Medium][Time Horizon: Operations Assessment]*

M.D.B.12. Each Planning Coordinator shall have dated evidence such as reports, data gathered from an historical event, or other dated documentation to show that it participated in a UFLS design assessment per Requirements D.B.12 and D.B.4 if UFLS program deficiencies are identified in D.B.11.

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
D.B.1	N/A	The Planning Coordinator participated in a joint regional review with the other Planning Coordinators in the WECC Regional Entity area that developed and documented criteria but failed to include the consideration of historical events, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas, that may form islands OR The Planning Coordinator participated in a joint regional review with the other Planning Coordinators in the WECC Regional Entity area that developed and documented criteria but failed to include the consideration of system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas, that may form islands	The Planning Coordinator participated in a joint regional review with the other Planning Coordinators in the WECC Regional Entity area that developed and documented criteria but failed to include the consideration of historical events and system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas, that may form islands	The Planning Coordinator failed to participate in a joint regional review with the other Planning Coordinators in the WECC Regional Entity area that developed and documented criteria to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas that may form islands

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
D.B.2	N/A	N/A	The Planning Coordinator identified an island(s) from the regional review to serve as a basis for designing its UFLS program but failed to include one (1) of the parts as specified in Requirement D.B.2, Parts D.B.2.1 or D.B.2.2	The Planning Coordinator identified an island(s) from the regional review to serve as a basis for designing its UFLS program but failed to include all of the parts as specified in Requirement D.B.2, Parts D.B.2.1 or D.B.2.2 OR The Planning Coordinator failed to identify any island(s) from the regional review to serve as a basis for designing its UFLS program.
D.B.3	N/A	The Planning Coordinator adopted a UFLS program, coordinated across the WECC Regional Entity area that included notification of and a schedule for implementation by UFLS entities within its area, but failed to meet one (1) of the performance characteristic in Requirement D.B.3, Parts D.B.3.1, D.B.3.2, or D.B.3.3 in	The Planning Coordinator adopted a UFLS program, coordinated across the WECC Regional Entity area that included notification of and a schedule for implementation by UFLS entities within its area, but failed to meet two (2) of the performance characteristic in Requirement D.B.3, Parts D.B.3.1, D.B.3.2, or D.B.3.3 in simulations of underfrequency conditions	The Planning Coordinator adopted a UFLS program, coordinated across the WECC Regional Entity area that included notification of and a schedule for implementation by UFLS entities within its area, but failed to meet all the performance characteristic in Requirement D.B.3, Parts D.B.3.1, D.B.3.2, and D.B.3.3 in

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
		simulations of underfrequency conditions		simulations of underfrequency conditions OR The Planning Coordinator failed to adopt a UFLS program, coordinated across the WECC Regional Entity area, including notification of and a schedule for implementation by UFLS entities within its area.
D.B.4	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators in the WECC Regional Entity area at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include one (1) of the items as specified in Requirement	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators in the WECC Regional Entity area at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include two (2) of the items as specified in	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators in the WECC Regional Entity area at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include three (3) of the items as specified in	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators in the WECC Regional Entity area at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2 but the simulation failed to include four (4) or more of the items as

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	D.B.4, Parts D.B.4.1 through D.B.4.7.	Requirement D.B.4, Parts D.B.4.1 through D.B.4.7.	Requirement D.B.4, Parts D.B.4.1 through D.B.4.7.	specified in Requirement D.B.4, Parts D.B.4.1 through D.B.4.7. OR The Planning Coordinator failed to participate in and document a coordinated UFLS assessment with the other Planning Coordinators in the WECC Regional Entity area at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement D.B.3 for each island identified in Requirement D.B.2
D.B.11	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event and	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event and	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event and

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	same islanding event and evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than one year but less than or equal to 13 months of actuation.	evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than 13 months but less than or equal to 14 months of actuation.	evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than 14 months but less than or equal to 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event within one year of event actuation but failed to evaluate one (1) of the parts as specified in Requirement D.B.11, Parts D.B.11.1 or D.B.11.2.	evaluated the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2 within a time greater than 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, failed to participate in and document a coordinated event assessment with all Planning Coordinators whose areas or portion of whose areas were also included in the same island event and evaluate the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, participated in and documented

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				a coordinated event assessment with all Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event within one year of event actuation but failed to evaluate all of the parts as specified in Requirement D.B.11, Parts D.B.11.1 and D.B.11.2.
D.B.12	N/A	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, participated in and documented a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators in the WECC Regional Entity area to consider the identified deficiencies in greater than two years but less than or equal to 25 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, participated in and documented a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators in the WECC Regional Entity area to consider the identified deficiencies in greater than 25 months but less than or equal to 26 months of event actuation.	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, participated in and documented a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators in the WECC Regional Entity area to consider the identified deficiencies in greater than 26 months of event actuation. OR The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement D.B.11, failed to participate in

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				and document a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators in the WECC Regional Entity area to consider the identified deficiencies

E. Associated Documents

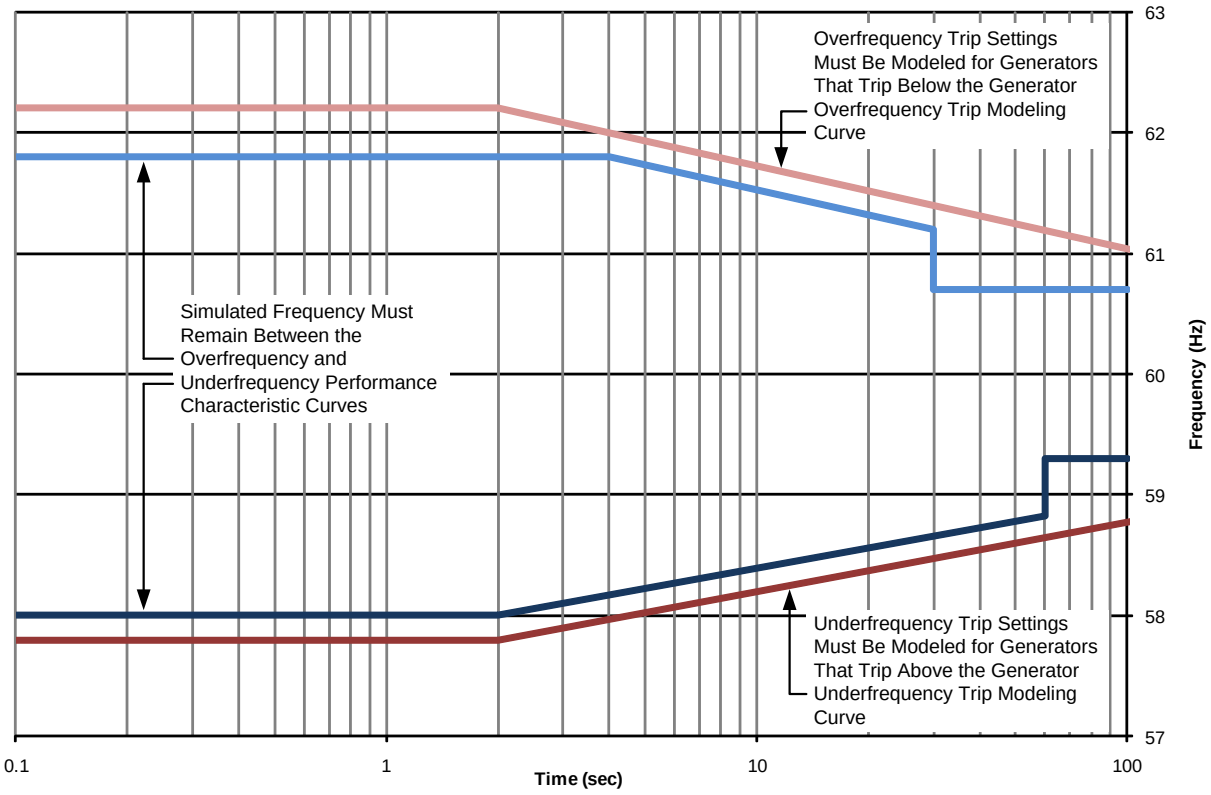
Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	May 25, 2010	Completed revision, merging and updating PRC-006-0, PRC-007-0 and PRC-009-0.	
1	November 4, 2010	Adopted by the Board of Trustees	
1	May 7, 2012	FERC Order issued approving PRC-006-1 (approval becomes effective July 10, 2012)	
1	November 9, 2012	FERC Letter Order issued accepting the modification of the VRF in R5 from (Medium to High) and the modification of the VSL language in R8.	
2	November 13, 2014	Adopted by the Board of Trustees	Revisions made under Project 2008-02: Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS) to address directive issued in FERC Order No. 763. Revisions to existing Requirement R9 and R10 and addition of new Requirement R15.
3	August 10, 2017	Adopted by the NERC Board of Trustees	Revisions to the Regional Variance for the Quebec Interconnection.
3	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the	Technical Rationale Initiative

		standard, the version number remains unchanged.	

PRC-006-3 – Attachment 1

Underfrequency Load Shedding Program
Design Performance and Modeling Curves for
Requirements R3 Parts 3.1-3.2 and R4 Parts 4.1-4.6

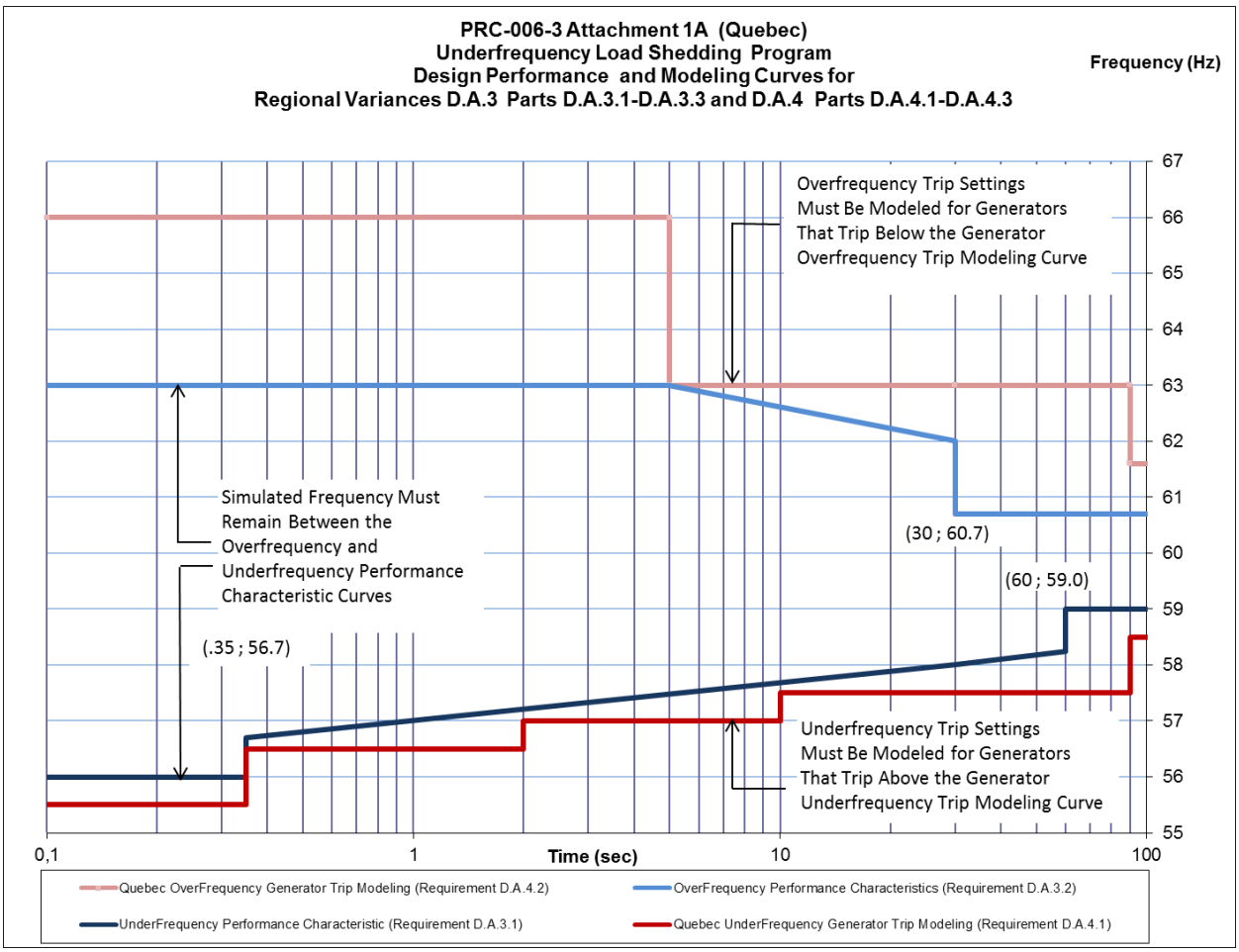


Generator Overfrequency Trip Modeling (Requirement R4 Parts 4.4-4.6)
Overfrequency Performance Characteristic (Requirement R3 Part 3.2)
Underfrequency Performance Characteristic (Requirement R3 Part 3.1)
Generator Underfrequency Trip Modeling (Requirement R4 Parts 4.1-4.3)

Curve Definitions

Generator Overfrequency Trip Modeling		Overfrequency Performance Characteristic		
t ≤ 2 s	t > 2 s	t ≤ 4 s	4 s < t ≤ 30 s	t > 30 s
f = 62.2 Hz	f = -0.686log(t) + 62.41 Hz	f = 61.8 Hz	f = -0.686log(t) + 62.21 Hz	f = 60.7 Hz

Generator Underfrequency Trip Modeling		Underfrequency Performance Characteristic		
t ≤ 2 s	t > 2 s	t ≤ 2 s	2 s < t ≤ 60 s	t > 60 s
f = 57.8 Hz	f = 0.575log(t) + 57.63 Hz	f = 58.0 Hz	f = 0.575log(t) + 57.83 Hz	f = 59.3 Hz


PRC-006-3 Attachment 1A (Quebec)
Underfrequency Load Shedding Program
Design Performance and Modeling Curves for
Regional Variances D.A.3 Parts D.A.3.1-D.A.3.3 and D.A.4 Parts D.A.4.1-D.A.4.3
Frequency (Hz)
Overfrequency Trip Settings
Must Be Modeled for Generators
That Trip Below the Generator
Overfrequency Trip Modeling Curve
Simulated Frequency Must
Remain Between the
Overfrequency and
Underfrequency Performance
Characteristic Curves
(.35 ; 56.7)
(30 ; 60.7)
(60 ; 59.0)
Underfrequency Trip Settings
Must Be Modeled for Generators
That Trip Above the Generator
Underfrequency Trip Modeling Curve
67
66
65
64
63
62
61
60
59
58
57
56
55
0,1
1
10
100
Time (sec)
Quebec OverFrequency Generator Trip Modeling (Requirement D.A.4.2)
OverFrequency Performance Characteristics (Requirement D.A.3.2)
UnderFrequency Performance Characteristic (Requirement D.A.3.1)
Quebec UnderFrequency Generator Trip Modeling (Requirement D.A.4.1)

~~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 R9:~~

~~The "Corrective Action Plan" language was added in response to the FERC directive from Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a Planning Coordinator (PC) assessment. The revised language adds clarity by requiring that each UFLS entity follow the UFLS program, including any Corrective Action Plan, developed by the PC.~~

~~Also, to achieve consistency of terminology throughout this standard, the word "application" was replaced with "implementation." (See Requirements R3, R14 and R15)~~

~~Rationale for R10:~~

~~The "Corrective Action Plan" language was added in response to the FERC directive from Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a PC assessment. The revised language adds clarity by requiring that each UFLS entity follow the UFLS program, including any Corrective Action Plan, developed by the PC.~~

~~Also, to achieve consistency of terminology throughout this standard, the word "application" was replaced with "implementation." (See Requirements R3, R14 and R15)~~

~~Rationale for R15:~~

~~Requirement R15 was added in response to the directive from FERC Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a PC assessment. Requirement R15 addresses the FERC directive by making explicit that if deficiencies are identified as a result of an assessment, the PC shall develop a Corrective Action Plan and schedule for implementation by the UFLS entities.~~

~~A "Corrective Action Plan" is defined in the NERC Glossary of Terms as, "a list of actions and an associated timetable for implementation to remedy a specific problem." Thus, the Corrective Action Plan developed by the PC will identify the specific timeframe for an entity to implement corrections to remedy any deficiencies identified by the PC as a result of an assessment.~~

Effective Date

Effective for SERC Region applicable Registered Entities on the first day of the first calendar quarter after approved by FERC.

Introduction

1. **Title:** Automatic Underfrequency Load Shedding Requirements

2. **Number:** PRC-006-SERC–02

3. **Purpose:** To establish consistent and coordinated requirements for the design, implementation, and analysis of automatic underfrequency load shedding (UFLS) programs among all SERC applicable entities.

4. **Applicability:**
   - **4.1** Planning Coordinators
   - **4.2** UFLS entities shall mean all entities that are responsible for the ownership, operation, or control of UFLS equipment as required by the UFLS program established by the Planning Coordinators. Such entities may include one or more of the following:
     - 4.2.1 Transmission Owners
     - 4.2.2 Distribution Providers
   - **4.3** Generator Owners

5. **Background**

   The SERC UFLS Standard: PRC-006-SERC-01 ("SERC UFLS Standard") was developed to provide regional UFLS requirements to entities in SERC. UFLS requirements have been in place at a continent-wide level and within SERC for many years prior to implementation of federally mandated reliability compliance standards in 2007.

   When reliability standards were implemented in 2007, the Federal Energy Regulatory Commission ("FERC"), which is the government body with regulatory responsibility for electric reliability, issued FERC Order 693, recognizing 83 NERC Reliability Standards as enforceable by FERC and applicable to users, owners, and operators of the bulk power system (BPS). FERC did not approve the NERC UFLS standard, PRC-006-0 in Order 693. FERC's reason for not approving PRC-006-0 was that it recognized PRC-006-0 as a "fill-in the blank standard," and regional procedures associated with the standard were not submitted along with the standard. FERC's ruling in Order 693 required Regional Entities to provide the regional requirements necessary for completing the UFLS standard.

   In 2008, SERC commenced work on PRC-006-SERC-01. NERC also began work on revising PRC-006-0 at a continent-wide level. The SERC standard has been developed to be consistent with the NERC UFLS standard. PRC-006-SERC-02 was developed per periodic review of the standard.
   PRC-006-1 clearly defines the roles and responsibilities of parties to whom the standard applies. The standard identifies the Planning Coordinator ("PC") as the entity responsible for developing UFLS schemes within their PC area. The regional standard adds specificity not contained in the NERC standard for development and implementation of a UFLS scheme in the SERC Region that effectively mitigates the consequences of an underfrequency event.

Requirements and Measures

R1. Each Planning Coordinator shall include its SERC subregion as an identified island in the criteria (required by the NERC PRC standard on UFLS) for selecting portions of the BPS that may form islands. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1 A Planning Coordinator may adjust island boundaries to differ from subregional boundaries where necessary for the sole purpose of producing a contiguous subregional island more suitable for simulation.

M1. Each Planning Coordinator shall have evidence such as a methodology, procedure, report, or other documentation indicating that its criteria included selection of its SERC subregion(s) as an island per Requirement R1.

R2. Each Planning Coordinator shall select or develop an automatic UFLS scheme (percent of load to be shed, frequency set points, and time delays) for implementation by UFLS entities within its area that meets the following minimum requirements: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. Have the capability of shedding at least 30 percent of the Peak Demand (MW) served from the Planning Coordinator's transmission system. The Peak Demand may be either summer or winter as determined by the Planning Coordinator.

2.2. Shed load with a minimum of three frequency set points.

2.3. The highest frequency set point for relays used to arrest frequency decline shall be no lower than 59.3 Hz and not higher than 59.5 Hz.

2.3.1 This does not apply to UFLS relays with time delay of one second or longer and a higher frequency setpoint applied to prevent the frequency from stalling at less than 60 Hz when recovering from an underfrequency event.

2.4. The lowest frequency set point shall be no lower than 58.4 Hz.

2.5. The difference between frequency set points shall be at least 0.2 Hz but no greater than 0.5 Hz.

2.6. Time delay (from frequency reaching the set point to the trip signal) shall be at least six cycles.

M2. Each Planning Coordinator shall have evidence such as reports or other documentation that the UFLS scheme for its area meets the design requirements specified in Requirement R2.

R3. Each Planning Coordinator, when performing design assessments specified in the NERC PRC standard on UFLS, shall conduct simulations of its UFLS scheme for an imbalance between load and generation of 13%, 22%, and 25% for all identified island(s) where such imbalance equals [(load minus actual generation output) / load]. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M3. Each Planning Coordinator shall have evidence such as reports or other documentation that it performed the simulations of its UFLS scheme as required in Requirement R3.

R4. Each UFLS entity that has a total load of 100 MW or greater in a Planning Coordinator area in the SERC Region shall implement the UFLS scheme developed by their Planning Coordinator. UFLS entities may implement the UFLS scheme developed by the Planning Coordinator by coordinating with other UFLS entities. The UFLS scheme shall meet the following requirements on May 1 of each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1. The percent of load shedding to be implemented shall be based on the actual or estimated substation or feeder demand (including losses) of the UFLS entities at the time coincident with the previous year's actual Peak Demand in the season specified by the Planning Coordinator in R2.

4. 2. The amount of load in each load shedding step shall be within -1.0 and +3.0 of the percentage specified by the Planning Coordinator (for example, if the specified percentage step load shed is 12%, the allowable range is 11 to 15%).

4. 3. The amount of total UFLS load of all steps combined shall be within -1.0 and +5.0 of the percentage specified by the Planning Coordinator for the total UFLS load in the UFLS scheme.

M4. Each UFLS entity that has a total load of 100 MW or greater in a Planning Coordinator area in the SERC Region shall have evidence such as reports or other documentation demonstrating that its implementation of the UFLS scheme on May 1 of each calendar year meets the requirements of Requirement R4 (including all the data elements in Parts 4.1, 4.2, and 4.3) unless scheme changes per Requirement R6 are in process.

R5. Each UFLS entity that has a total load less than 100 MW in a Planning Coordinator area in the SERC Region shall implement the UFLS scheme developed by their Planning Coordinator, but shall not be required to have more than one UFLS step. UFLS entities may implement the UFLS scheme developed by the Planning Coordinator by coordinating with other UFLS entities. The UFLS scheme shall meet the following requirements on May 1 of each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

5.1. The percent of load shedding to be implemented shall be based on the actual or estimated substation or feeder demand (including losses) of the UFLS entities at the time coincident with the previous year actual Peak Demand in the season specified by the Planning Coordinator in R2..

5.2. The amount of total UFLS load shall be within ± 5.0 of the percentage specified by the Planning Coordinator for the total UFLS load in the UFLS scheme.

M5. Each UFLS entity that has a total load less than 100 MW in a Planning Coordinator area in the SERC Region shall have evidence such as reports or other documentation demonstrating that its implementation of the UFLS scheme on May 1 of each calendar year meets the requirements of Requirement R5 (including all the data elements in Parts 5.1and 5.2) unless scheme changes per Requirement R6 are in process.

R6. Each UFLS entity shall implement changes to the UFLS scheme which involve frequency settings, relay time delays, changes to the percentage of load in the scheme, or changes to the peak season selected in R2.1 within 18 months of notification by the Planning Coordinator. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M6. Each UFLS entity shall have evidence such as reports or other documentation demonstrating that it has made the appropriate scheme changes within 18 months per Requirement R6. Such evidence is only required if the Planning Coordinator makes changes to the UFLS scheme as specified in Requirement R6.

R7. Each Planning Coordinator shall provide the following information to SERC according to the schedule specified by SERC. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

7.1. Underfrequency trip set points (Hz)

7.2. Total clearing time associated with each set point (sec). This includes the time from when frequency reaches the set point and ends when the breaker opens.

7.3. Amount of previous year actual or estimated load associated with each set point, both in percent and in MW. The percentage and the Load demand (MW) shall be based on the time coincident with the previous year actual Peak Demand.

M7. Each Planning Coordinator shall have evidence such as reports or other documentation that data specified in Requirement R7 was provided to SERC in accordance with the schedule.

R8. Each Generator Owner shall provide the following information within 30 days of a request by SERC to facilitate post-event analysis of frequency disturbances. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

8.1. Generator protection automatic underfrequency and overfrequency trip set points (Hz).

8.2. Total clearing time associated with each set point (sec). This is defined as the time that begins when frequency reaches the set point and ends when the breaker opens. If inverse time underfrequency relays are used, provide the total clearing time at 59.0, 58.5, 58.0, and 57.0 Hz.

8.3. Maximum generator net MW that could be tripped automatically due to an underfrequency or overfrequency condition.

M8. Each Generator Owner shall have evidence such as reports or other documentation that data specified in Requirement R8 was provided to SERC as requested.

Compliance

Compliance enforcement authority

SERC Reliability Corporation

Compliance monitoring and assessment process

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Violation Investigation
- Self-Reporting
- Complaint

Evidence retention

Each Planning Coordinator, UFLS Entity and Generator Owner shall keep data or evidence to show compliance as identified below unless directed by SERC to retain specific evidence for a longer period of time as part of an investigation.

Each Planning Coordinator, UFLS Entity and Generator Owner shall retain the current evidence of each Requirement and Measure as well as any evidence necessary to show compliance since the last compliance audit.

If a Planning Coordinator, UFLS Entity or Generator Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the retention period specified above, whichever is longer.

The compliance enforcement authority shall keep the last audit records and all requested and submitted subsequent audit records.

Time Horizons, Violation Risk Factors, and Violation Severity Levels

Table 1						
R#	Time Horizon	VRF	Violation Severity Level			
			Lower	Moderate	High	Severe
R1	Long-term Planning	Medium	N/A	N/A	N/A	The Planning Coordinator did not have evidence that its criteria included selection of its SERC subregion(s) as an island, with or without adjusted boundaries.
R2	Long-term Planning	Medium	The Planning Coordinator's scheme did not meet one of the UFLS system design requirements identified in 2.2 through 2.6	The Planning Coordinator's scheme did not meet two of the UFLS system design requirements identified in 2.2 through 2.6.	The Planning Coordinator's scheme did not meet three of the UFLS system design requirements identified in 2.2 through 2.6.	The Planning Coordinator's scheme did not meet 2.1 **OR** Four or more of the UFLS system design requirements identified in 2.2 through 2.6.
R3	Long-term Planning	High	N/A	The Planning Coordinator failed to conduct one of the required simulations of its UFLS scheme.	N/A	The Planning Coordinator failed to conduct two of the required simulations of its UFLS scheme.
R4	Operations Planning	Medium	The UFLS entity's implemented UFLS scheme had one load shedding step outside the range specified in 4.	The UFLS entity's implemented UFLS scheme had two load shedding steps outside the range specified in 4.	The UFLS entity's implemented UFLS scheme had three or more load shedding steps outside the range	The UFLS entity's implemented UFLS scheme had three or more load shedding steps outside the range

Table 1						
R#	Time Horizon	VRF	Violation Severity Level			
			Lower	Moderate	High	Severe
			2.	2.	specified in 4.2. **OR** The UFLS entity's implemented UFLS scheme had a total load outside the range specified in 4.3.	specified in 4.2. **AND** The UFLS entity's implemented UFLS scheme had a total load outside the range specified in 4.3.
R5	Operations Planning	Medium	N/A	N/A	N/A	The UFLS entity's implemented UFLS scheme had a total load outside the range specified in 5.2.
R6	Long-term Planning	High	The UFLS entity implemented required scheme changes but made them 1 to 30 days after the scheduled date.	The UFLS entity implemented required scheme changes but made them 31 to 40 days after the scheduled date.	The UFLS entity implemented required scheme changes but made them 41 to 50 days after the scheduled date.	The UFLS entity implemented required scheme changes but made them more than 50 days after the scheduled date OR The UFLS entity failed to implement the required scheme changes.
R7	Long-term Planning	Lower	The Planning Coordinator provided the data required in R7 to SERC 1 to 10 days	The Planning Coordinator provided the data required in R7 to SERC 11 to 20 days	The Planning Coordinator provided the data required in R7 to SERC 21 to 30 days	The Planning Coordinator provided the data required in R7 to SERC more than 30

Table 1						
R#	Time Horizon	VRF	Violation Severity Level			
			Lower	Moderate	High	Severe
			after the scheduled submittal date.	after the scheduled submittal date. **OR** The Planning Coordinator did not provide to SERC one piece of information listed in R7.	after the scheduled submittal date. **OR** The Planning Coordinator did not provide to SERC two pieces of information listed in R7.	days after the scheduled submittal date. **OR** The Planning Coordinator did not provide to SERC any of the information listed in R7.
R8	Long-term Planning	Lower	The Generator Owner provided the data required in R8 to SERC 1 to 10 days after the requested submittal date.	The Generator Owner provided the data required in R8 to SERC 11 to 20 days after the requested submittal date. **OR** The Generator Owner did not provide to SERC one piece of information listed in R8.	The Generator Owner provided the data required in R8 to SERC 21 to 30 days after the requested submittal date. **OR** The Generator Owner did not provide to SERC two pieces of information listed in R8.	The Generator Owner provided the data required in R8 to SERC more than 30 days after the requested submittal date. **OR** The Generator Owner did not provide to SERC any of the information listed in R8.

Regional Variances

None

Interpretations

None

~~Guideline and Technical Basis~~

~~1. Existing UFLS schemes~~

~~Each Planning Coordinator should consider the existing UFLS programs which are in place and should consider input from the UFLS entities in developing the UFLS scheme.~~

~~2. Basis for SERC standard requirements~~

~~SERC Standard PRC-006-SERC-02 is not a stand-alone standard, but was written to be followed in conjunction with NERC Standard PRC-006-1. The primary focus of SERC Standard PRC-006-SERC-02 was to provide region-specific requirements for the implementation of the higher tier NERC standard requirements with the goals of a) adding clarity and b) providing for consistency and a coordinated UFLS scheme for the SERC Region as a whole.~~
~~Generally speaking, requirements already in the NERC standard were not repeated in the SERC standard. Therefore, both the NERC and SERC standards must be followed to ensure full compliance.~~

~~3. Basis for applying a percentage load shedding value to Forecast Load versus Actual Load~~

~~The Planning Coordinator will develop a UFLS scheme to meet the performance requirements of NERC Standard PRC-006-2 Requirement R3 and SERC Standard PRC-006-SERC-02 Requirement R2. This development will result in certain percentages of load for each UFLS entity in the Planning Coordinator's area for which automatic under frequency load shedding must be implemented. The Planning Coordinator develops these percentages based on forecast peak load demand. However, the UFLS entity implements these percentages based on the previous year's actual peak demand. Applying the same percentage to these different base values was intentional to ensure that both the Planning Coordinator and UFLS entities had a clear, measurable value to use in performing their respective roles in meeting the standard. Planning Coordinators typically use forecast demands in their work. Whereas the previous year's actual (or estimated) demand is typically more available to UFLS entities. Additionally, the use of percentages based on these different base values tends to minimize the error due to the time lag between design and actual field implementation. Since a percentage is provided by the Planning Coordinator to the UFLS entities, any differences between the design values (i.e., forecast load) and the implemented values (i.e., previous year's actual) would naturally tend to match up reasonably well. For example, if the total planning area load in MW for which UFLS was installed during the time of implementation was slightly higher or lower than the MW value used in the design by the Planning Coordinator, multiplying by the specified percentage would result in an implemented load shedding scheme that also had a reasonably similar higher or lower MW value.~~

4. Basis for May 1 and 18 month time frames

Each UFLS entity must annually review that the amount of UFLS load shedding implemented is within a certain tolerance as specified by SERC Standard PRC-006-SERC-02 Requirement R 4 or Requirement R5 by May 1 of the current year. May 1 was chosen to allow sufficient time after the previous year's peak occurred to make adjustments in the field to the implementation if necessary to meet the tolerances specified in Requirement R4 or Requirement R5. Therefore, the May 1 date applies only to implementation of the existing percentages of load shedding specified by the Planning Coordinator. On the other hand, the 18-month time frame specified in PRC-006-SERC-02 Requirement R6 is intended to allow sufficient budgeting, procurement, and installation time for additional equipment, or for significant setting changes to existing equipment necessary to meet a revised load shedding scheme design that has been specified by the Planning Coordinator. During this 18-month transition period, the May 1 measurement of R4 or Requirement R5 would not apply.

5. Basis for smaller entity threshold of 100 MW

Most distribution substations have transformers rated in the range of 10 to 40 MVA. Usually most transformers would serve 1 to 4 feeders and each feeder will normally carry between 8 and 10 MVA. In general, assuming that each feeder would carry 10 MW, an entity with a load slightly greater than 100 MW would have at least 10 feeders available. For a program with three 10 % steps, only 3 feeders would be required to have under frequency load shed capabilities. The 100 MW threshold seems to provide adequate flexibility for implementing load shedding in three steps for entities slightly greater than 100 MW.

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 each of the rationale text boxes was moved to this section.

Rationale for R1:

Studying the Region as an island is required by the NERC standard. Most regions have only one or a few different UFLS schemes. Where there is more than one scheme, studying this island demonstrates that the schemes are coordinated and performing adequately. Because there are so many different UFLS schemes in SERC (18 different schemes were represented in the 2007 SERC UFLS study), the SDT believes that applying the schemes to each subregion as an island is a necessary additional test of the coordination of the various UFLS schemes. Without this additional test, a poorly performing scheme may be masked by the large number of good performing schemes in the Region. A subregion island study, which would have a smaller number of schemes, would be more likely to uncover the poorly performing scheme and therefore get it fixed. This approach will result in a much better overall performance of the UFLS programs in SERC. The SDT recognized that there may be simulation problems due to opening the ties to utilities outside the subregion. Therefore, the subregion island boundaries are allowed to be adjusted to produce an island more suitable for simulation.

~~(Note: The SERC Subregions are identified in paragraph 4.2 of the SERC Reliability Corporation Bylaws: "The Region is currently geographically divided into five subregions that are identified as Southeastern, Central, VACAR, Delta, and Gateway.")~~

~~Rationale for R2:~~

~~These requirements for the UFLS schemes in SERC have been in place for many years (except 2.6). The SDT believes that these requirements are still needed to ensure consistency for the various schemes which are used in SERC. Part 2.6 is designed to prevent spurious operations due to transient frequency swings.~~

~~Rationale for R3:~~

~~R4 of the NERC standard PRC-006-1 requires the PC to conduct assessments of UFLS schemes through dynamic simulations to verify that they meet performance requirements for generation/load imbalances of up to 25%. This requirement defines specific imbalances that are to be studied within SERC. The 13% and 22% levels were determined from simulations of the worst case frequency overshoot for the UFLS schemes in SERC.~~

~~Rationale for R4:~~

~~The SDT believes it is necessary to put a requirement on how well the UFLS scheme is implemented. This requirement specifies how close the actual load shedding amounts must be to the percentage of load called for in the scheme. A 4 percentage point range is allowed for each individual step, but the allowed range for all steps combined is 6 percentage points.~~

~~Rationale for R5:~~

~~The SDT believes it is necessary to put a requirement on how well the UFLS scheme is implemented. This requirement specifies how close the actual load shedding amounts must be to the percentage of load called for in the scheme. The SDT recognizes that UFLS entities with a load of less than 100 MW may have difficulty in implementing more than one UFLS step and in meeting a tight tolerance. The basis of the 100 MW comes from typical feeder load dropped by UFLS relays, and the use of a 100 MW threshold in other regional UFLS standards.~~

~~Rationale for R6:~~

~~The SDT believes it is necessary to put a requirement on how quickly changes to the scheme should be implemented. This requirement specifies that changes must be implemented within 18 months of notification by the PC. The 18 month interval was chosen to give a reasonable amount of time for making changes in the field. All of the SERC Region has existing UFLS schemes which, based on periodic simulations, have provided reliable protection for years. Events which result in islanding and an activation of the UFLS schemes are extremely rare in SERC. Therefore, the SDT does not believe that changes to an existing UFLS scheme will be needed in less than 18 months. However, if a PC determines there is a need for changing the UFLS scheme faster than 18 months, then the PC may require the implementation to be done sooner as allowed by NERC Reliability Standard PRC-006-1.~~

~~**Rationale for R7:**~~

~~The NERC standard requires that a UFLS database be maintained by the Planning Coordinator. This requirement specifies what data must be reported to SERC. A SERC UFLS database is needed to facilitate data sharing across the SERC Region, with other regions, and with NERC.~~

~~**Rationale for R8:**~~

~~The SDT believes that generator over and under frequency tripping data is needed to supplement the UFLS data provided by the Planning Coordinator for post-event analysis of frequency disturbances. This requirement states what data must be reported to SERC by the Generator Owners.~~

~~Since the inverse time curve cannot easily be placed into the SERC database, four clearing times based on data from the curve are requested. These clearing times are intended to cover a range of frequencies needed for event replication as well as provide information about generators that trip at a higher frequency than is allowed by the NERC standard.~~

Version History

Version	Date	Action	Change Tracking
1	September 19, 2011	SERC Board Approved	
1	November 3, 2011	Adopted by NERC Board of Trustees	
1	December 20, 2012	FERC Order issued approving PRC-006-SERC–01	
1	March 11, 2013	Modified the Rationale and changed the VRF for Requirement R6 from “Medium” to “High” per a compliance filing (Filed on 3/11/13)	
2	June 28, 2017	SERC Board Approved	
2	August 10, 2017	Adopted by NERC Board of Trustees	
2	October 16, 2017	FERC Order issued approving PRC-006-SERC-02	
2	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

A. Introduction

1. **Title: Operations Planning**
2. **Number: TOP-002-4**
3. **Purpose:** To ensure that Transmission Operators and Balancing Authorities have plans for operating within specified limits.
4. **Applicability:**
   - **4.1.** Transmission Operator
   - **4.2.** Balancing Authority
5. **Effective Date:**

   See Implementation Plan.
6. **Background:**

   See Project 2014-03 project page.

B. Requirements and Measures

R1. Each Transmission Operator shall have an Operational Planning Analysis that will allow it to assess whether its planned operations for the next day within its Transmission Operator Area will exceed any of its System Operating Limits (SOLs). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Each Transmission Operator shall have evidence of a completed Operational Planning Analysis. Such evidence could include but is not limited to dated power flow study results.

R2. Each Transmission Operator shall have an Operating Plan(s) for next-day operations to address potential System Operating Limit (SOL) exceedances identified as a result of its Operational Planning Analysis as required in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Each Transmission Operator shall have evidence that it has an Operating Plan to address potential System Operating Limits (SOLs) exceedances identified as a result of the Operational Planning Analysis performed in Requirement R1. Such evidence could include but it is not limited to plans for precluding operating in excess of each SOL that was identified as a result of the Operational Planning Analysis.

R3. Each Transmission Operator shall notify entities identified in the Operating Plan(s) cited in Requirement R2 as to their role in those plan(s). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Transmission Operator shall have evidence that it notified entities identified in the Operating Plan(s) cited in Requirement R2 as to their role in the plan(s). Such evidence could include but is not limited to dated operator logs, or e-mail records.

R4. Each Balancing Authority shall have an Operating Plan(s) for the next-day that addresses: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1 Expected generation resource commitment and dispatch

4.2 Interchange scheduling

4.3 Demand patterns

4.4 Capacity and energy reserve requirements, including deliverability capability

M4. Each Balancing Authority shall have evidence that it has developed a plan to operate within the criteria identified. Such evidence could include but is not limited to dated operator logs or e-mail records.

R5. Each Balancing Authority shall notify entities identified in the Operating Plan(s) cited in Requirement R4 as to their role in those plan(s). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Each Balancing Authority shall have evidence that it notified entities identified in the plan(s) cited in Requirement R4 as to their role in the plan(s). Such evidence could include but is not limited to dated operator logs or e-mail records.

R6. Each Transmission Operator shall provide its Operating Plan(s) for next-day operations identified in Requirement R2 to its Reliability Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. Each Transmission Operator shall have evidence that it provided its Operating Plan(s) for next-day operations identified in Requirement R2 to its Reliability Coordinator. Such evidence could include but is not limited to dated operator logs or e-mail records.

R7. Each Balancing Authority shall provide its Operating Plan(s) for next-day operations identified in Requirement R4 to its Reliability Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M7. Each Balancing Authority shall have evidence that it provided its Operating Plan(s) for next-day operations identified in Requirement R4 to its Reliability Coordinator. Such evidence could include but is not limited to dated operator logs or e-mail records.

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. Compliance Monitoring and Assessment Processes

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" 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. Data Retention

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

Each Transmission Operator and Balancing Authority shall keep data or evidence to show compliance for each applicable Requirement for a rolling 90-calendar days period for analyses, the most recent 90-calendar days for voice recordings, and 12 months for operating logs and e-mail records unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Transmission Operator or Balancing Authority is found non-compliant, it shall keep information related to the non-compliance until found compliant 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. Additional Compliance Information

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	N/A	N/A	The Transmission Operator did not have an Operational Planning Analysis allowing it to assess whether its planned operations for the next day within its Transmission Operator Area exceeded any of its System Operating Limits (SOLs).
R2	Operations Planning	Medium	N/A	N/A	N/A	The Transmission Operator did not have an Operating Plan to address potential System Operating Limit (SOL) exceedances identified as a result of the Operational Planning Analysis performed in Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
For the Requirement R3 and R5 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	Medium	The Transmission Operator did not notify one impacted entity or 5% or less of the entities, whichever is greater identified in the Operating Plan(s) as to their role in the plan(s).	The Transmission Operator did not notify two entities or more than 5% and less than or equal to 10% of the impacted entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	The Transmission Operator did not notify three impacted entities or more than 10% and less than or equal to 15% of the entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	The Transmission Operator did not notify four or more entities or more than 15% of the impacted NERC identified in the Operating Plan(s) as to their role in the plan(s).
R4	Operations Planning	Medium	The Balancing Authority has an Operating Plan but it does not address one of the criteria in Requirement R4.	The Balancing Authority has an Operating Plan but it does not address two of the criteria in Requirement R4.	The Balancing Authority has an Operating Plan but it does not address three of the criteria in Requirement R4.	The Balancing Authority did not have an Operating Plan.
R5	Operations Planning	Medium	The Balancing Authority did not notify one impacted entity or 5% or less	The Balancing Authority did not notify two entities or more than 5% and	The Balancing Authority did not notify three impacted entities or	The Balancing Authority did not notify four or more entities or more than

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	less than or equal to 10% of the impacted entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	more than 10% and less than or equal to 15% of the entities, whichever is greater, identified in the Operating Plan(s) as to their role in the plan(s).	15% of the impacted entities identified in the Operating Plan(s) as to their role in the plan(s).
R6	Operations Planning	Medium	N/A	N/A	N/A	The Transmission Operator did not provide its Operating Plan(s) for next-day operations as identified in Requirement R2 to its Reliability Coordinator.
R7	Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority did not provide its Operating Plan(s) for next-day operations as identified in Requirement R4 to its Reliability Coordinator.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Operating Plan - An Operating Plan includes general Operating Processes and specific Operating Procedures. It may be an overview document which provides a prescription for an Operating Plan for the next-day, or it may be a specific plan to address a specific SOL or IROL exceedance identified in the Operational Planning Analysis (OPA). Consistent with the NERC definition, Operating Plans can be general in nature, or they can be specific plans to address specific reliability issues. The use of the term Operating Plan in the revised TOP/IRO standards allows room for both. An Operating Plan references processes and procedures which are available to the System Operator on a daily basis to allow the operator to reliably address conditions which may arise throughout the day. It is valid for tomorrow, the day after, and the day after that. Operating Plans should be augmented by temporary operating guides which outline prevention/mitigation plans for specific situations which are identified day-to-day in an OPA or a Real-time Assessment (RTA). As the definition in the Glossary of Terms states, a restoration plan is an example of an Operating Plan. It contains all the overarching principles that the System Operator needs to work his/her way through the restoration process. It is not a specific document written for a specific blackout scenario but rather a collection of tools consisting of processes, procedures, and automated software systems that are available to the operator to use in restoring the system. An Operating Plan can in turn be looked upon in a similar manner. It does not contain a prescription for the specific set-up for tomorrow but contains a treatment of all the processes, procedures, and automated software systems that are at the operator's disposal. The existence of an Operating Plan, however, does not preclude the need for creating specific action plans for specific SOL or IROL exceedances identified in the OPA. When a Reliability Coordinator performs an OPA, the analysis may reveal instances of possible SOL or IROL exceedances for pre- or post-Contingency conditions. In these instances, Reliability Coordinators are expected to ensure that there are plans in place to prevent or mitigate those SOLs or IROLs, should those operating conditions be encountered the next day. The Operating Plan may contain a description of the process by which specific prevention or mitigation plans for day-to-day SOL or IROL exceedances identified in the OPA are handled and communicated. This approach could alleviate any potential administrative burden associated with perceived requirements for continual day-to-day updating of "the Operating Plan document" for compliance purposes.

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	August 2, 2006	Adopted by Board of Trustees	Revised
2	November 1, 2006	Adopted by Board of Trustees	Revised
2	June 14, 2007	Fixed typo in R11., (subject to …)	Errata
2a	February 10, 2009	Added Appendix 1 – Interpretation of R11 approved by BOT on February 10, 2009	Interpretation
2a	December 2, 2009	Interpretation of R11 approved by FERC on December 2, 2009	Same Interpretation
2b	November 4, 2010	Added Appendix 2 – Interpretation of R10 adopted by the Board of Trustees	
2b	October 20, 2011	FERC Order issued approving the Interpretation of R10 (FERC's Order became effective on October 20, 2011)	
2.1b	March 8, 2012	Errata adopted by Standards Committee; (Removed unnecessary language from the Effective Date section. Deleted retired sub-requirements from Requirement R14)	Errata
2.1b	April 11, 2012	Additional errata adopted by Standards Committee; (Deleted language from retired sub-requirement from Measure M7)	Errata
2.1b	September 13, 2012	FERC approved	Errata
3	May 6, 2012	Revisions under Project 2007-03	Revised

3	May 9, 2012	Adopted by Board of Trustees	Revised
4	April 2014	Revisions under Project 2014-03	Revised
4	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
4	November 19, 2015	FERC approved TOP-002-4. Docket No. RM15-16-000. Order No. 817.	
4	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

~~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:~~

~~Terms deleted in Requirement R1 as they are now contained in the revised definition of Operational Planning Analysis~~

~~Rationale for R2:~~

~~The change to Requirement R2 is in response to NOPR paragraph 42 and in concert with proposed changes made to proposed TOP-001-4~~

~~Rationale for R3:~~

~~Changes in response to IERP recommendation~~

~~Rationale for R4 and R5:~~

~~These Requirements were added to address IERP recommendations~~

~~Rationale for R6 and R7:~~

~~Added in response to SW Outage Report recommendation 1~~

A. Introduction

1. **Title: Operational Reliability Data**

2. **Number: TOP-003-3**

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. Load-Serving Entity

   4.6. Transmission Owner

   4.7. Distribution Provider

5. **Effective Date:**

   See Implementation Plan.

6. **Background:**

   See Project 2014-03 project page.

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: Low] [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 status or degradation that impacts System reliability.

1.3. A periodicity for providing data.

1.4. 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: Low] [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 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 Assessment. *[Violation Risk Factor: Low] [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: Low] [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, Load-Serving Entity, 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, Load-Serving Entity, 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 Monitoring Process

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. Compliance Monitoring and Assessment Processes

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" 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. Data Retention

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

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, Load-Serving Entity, 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. 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	The Transmission Operator did not include one of the parts (Part 1.1 through Part 1.4) 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 of the parts (Part 1.1 through Part 1.4) 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 three of the parts (Part 1.1 through Part 1.4) 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 of the parts (Part 1.1 through Part 1.4) 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	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	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 to10% 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	Low	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	
3	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed	Technical Rationale Initiative

		and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	

~~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.~~

A. Introduction

1. **Title:** **Real-time Reliability Monitoring and Analysis Capabilities**
2. **Number:** **TOP-010-1(i)**
3. **Purpose:** Establish requirements for Real-time monitoring and analysis capabilities to support reliable System operations.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Transmission Operators
     - **4.1.2.** Balancing Authorities
5. **Effective Date:** See Implementation Plan

B. Requirements and Measures

R1. Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

- **1.1.** Criteria for evaluating the quality of Real-time data;
- **1.2.** Provisions to indicate the quality of Real-time data to the System Operator; and
- **1.3.** Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.

M1. Each Transmission Operator shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R1; and 2) evidence the Transmission Operator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R2. Each Balancing Authority shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

- **2.1.** Criteria for evaluating the quality of Real-time data;
- **2.2.** Provisions to indicate the quality of Real-time data to the System Operator; and

2.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects its analysis functions.

M2. Each Balancing Authority shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R2; and 2) evidence the Balancing Authority implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R3. Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

3.1. Criteria for evaluating the quality of analysis used in its Real-time Assessments;

3.2. Provisions to indicate the quality of analysis used in its Real-time Assessments; and

3.3. Actions to address analysis quality issues affecting its Real-time Assessments.

M3. Each Transmission Operator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments as specified in Requirement R3. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R3; and 2) evidence the Transmission Operator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R4. Each Transmission Operator and Balancing Authority shall have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. Each Transmission Operator and Balancing Authority shall have evidence of an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. This evidence could include, but is not limited to, operator logs, computer printouts, system specifications, or other evidence.

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 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 applicable entity shall retain evidence of compliance for Requirements R1, R2, and R4, and Measures M1, M2, and M4 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, 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 evidence of compliance for Requirement R3 and Measure M3 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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.

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 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	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include one of the elements listed in Part 1.1 through Part 1.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include two of the elements listed in Part 1.1 through Part 1.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include any of the elements listed in Part 1.1 through Part 1.3; OR The Transmission Operator did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments.
R2.	N/A	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the

		Real-time data necessary to perform its analysis functions and Real-time monitoring did not include one of the elements listed in Part 2.1 through Part 2.3.	Real-time data necessary to perform its analysis functions and Real-time monitoring did not include two of the elements listed in Part 2.1 through Part 2.3.	Real-time data necessary to perform its analysis functions and Real-time monitoring did not include any of the elements listed in Part 2.1 through Part 2.3; OR The Balancing Authority did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring.
R3.	N/A	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include one of the elements listed in Part 3.1 through Part 3.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include two of the elements listed in Part 3.1 through Part 3.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include any of the elements listed in Part 3.1 through Part 3.3; OR The Transmission Operator did not implement an Operating Process or Operating Procedure to address the quality of

				analysis used in its Real-time Assessments.
R4.	N/A	N/A	The responsible entity has an alarm process monitor but the alarm process monitor did not provide notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor occurred.	The responsible entity does not have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	October 30, 2015	New standard developed in Project 2009-02 to respond to recommendations in Real-time Best Practices Task Force Report and FERC directives.	N/A
1	May 5, 2016	Adopted by the Board of Trustees	New
1	September 22, 2016	FERC Order issued approving TOP-010-1. Docket No. RD16-6-000	

1(i)	September 22, 2016	FERC directive to change Requirement 1 and Requirement 2 from 'medium' to 'high'. Docket No. RD16-6-000	Revised
1(i)	November 2, 2016	Adopted by the Board of Trustees	New
1(i)	December 14, 2016	FERC letter Order approving revisions to the VRF for R1 and R2 from 'medium' to 'high'. Docket No. RD16-6-001.	
1(i)	April 20, 2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

Supplemental Material

Guidelines and Technical Basis

Real-time monitoring, or *monitoring* the Bulk Electric System (BES) in Real-time, is a primary function of Reliability Coordinators (RCs), Transmission Operators (TOPs), and Balancing Authorities (BAs) as required by TOP and IRO Reliability Standards. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. Real-time monitoring may include the following activities performed in Real-time:

- Acquisition of operating data;
- Display of operating data as needed for visualization of system conditions;
- Audible or visual alerting when warranted by system conditions; and
- Audible or visual alerting when monitoring and analysis capabilities degrade or become unavailable.

Requirement R1

The TOP uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform monitoring and Real-time Assessments appear in other Reliability Standards.

The TOP's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R1 Part 1.1. The criteria support identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 specifies the TOP shall include actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments. Requirement R1 Part 1.3 is focused on addressing data point quality issues affecting Real-time Assessments. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R1 Part 1.3.

The TOP's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the TOP to meet its obligations for performing the Real-time Assessment. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the TOP;
- Following processes established for resolving data conflicts as specified in TOP-003-3, or other applicable Reliability Standards;
- Taking corrective actions on the TOP's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the TOP's Real-time Assessment; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the quality of the Real-time Assessment so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R2

The BA uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The BA's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R2 Part 2.1. The criteria supports identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 specifies the BA shall include in its Operating Process or Operating Procedure actions to address Real-time data quality issues when data quality affects its analysis functions. Requirement R2 Part 2.3 is focused on addressing data point quality issues affecting analysis functions. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R2 Part 2.3.

The BA's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the BA to meet its obligations for performing its analysis functions. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the BA;

- Following processes established for resolving data conflicts as specified in TOP-003-3 or other applicable Reliability Standards;
- Taking corrective actions on the BA's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the BA's analysis functions; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the analysis quality so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R3

Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments may include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

Examples of the types of criteria used to evaluate the quality of analysis used in Real-time Assessments may include solution tolerances, mismatches with Real-time data, convergences, etc.

The Operating Process or Operating Procedure must describe how the quality of analysis results used in Real-time Assessment will be shown to operating personnel.

Requirement R4

Requirement R4 addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

An alarm process monitor could be an application within a Real-time monitoring system or it could be a separate system. 'Heartbeat' or 'watchdog' monitors are examples of an alarm process monitor. An alarm process monitor should be designed and implemented such that a stall of the Real-time monitoring alarm processor does not cause a failure of the alarm process monitor.

Rationale

Rationale for Requirement R1: The Transmission Operator (TOP) uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform Real-time monitoring and Real-time Assessments appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 of this standard specifies the TOP shall include actions to address Real-time data quality issues affecting its Real-time Assessments in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process used to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2, provided that this process addresses Real-time data quality issues.

The revision in Part 1.3 to address Real-time data quality issues *when data quality affects Real-time Assessments* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R2: The Balancing Authority (BA) uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 of this standard specifies the BA shall include actions to address Real-time data quality issues affecting its analysis functions in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2 provided that this process addresses Real-time data quality issues.

The revision in Part 2.3 to address Real-time data quality issues *when data quality affects its analysis functions* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R3: Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments include, as applicable, state

estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

The Operating Process or Operating Procedure must include provisions for how the quality of analysis results used in Real-time Assessment will be shown to operating personnel. Operating personnel includes System Operators and staff responsible for supporting Real-time operations.

Rationale for Requirement R4: The requirement addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

The requirement in Draft Two of the proposed standard has been revised for clarity by removing the term *independent*. The alarm process monitor must be able to provide notification of failure of the Real-time monitoring alarm processor. This capability could be provided by an application within a Real-time monitoring system or by a separate component used by the System Operator. The alarm process monitor must not fail with a simultaneous failure of the Real-time monitoring alarm processor.

A. Introduction

1. **Title:** Power System Stabilizer (PSS)
2. **Number:** VAR-501-WECC-3.1
3. **Purpose:** To ensure the Western Interconnection is operated in a coordinated manner under normal and abnormal conditions by establishing the performance criteria for WECC power system stabilizers.
4. **Applicability:**
   - **4.1** Generator Operator
   - **4.2** Generator Owner
5. **Facilities:** This standard applies to synchronous generators, connected to the Bulk Electric System, that meet the definition of Commercial Operation.
6. **Effective Date:** The first day of the first quarter following regulatory approval, except for Requirement R3.

   For units placed in first-time service after regulatory approval, Requirement R3 is effective the first day of the first quarter following final regulatory approval.

   For units placed in service prior to final regulatory approval, Requirement R3 is effective the first day of the first quarter that is five years after regulatory approval.

B. Requirements and Measures

R1. Each Generator Owner shall provide to its Transmission Operator, the Generator Owner's written Operating Procedure or other document(s) describing those known circumstances during which the Generator Owner's PSS will not be providing an active signal to the Automatic Voltage Regulator (AVR), within 180 days of any of the following events: *[Violation Risk Factor: Low] [Time Horizon: Planning Horizon]*

- The effective date of this standard;
- The PSS's Commercial Operation date; or
- Any changes to the PSS operating specifications.

M1. Each Generator Owner will have documented evidence that it provided to its Transmission Operator, within the time allotted as described in the procedures required under Requirement R1, written Operating Procedures or other document(s) describing those known circumstances during which the Generator Owner's PSS will not be providing an active signal to the AVR.

For auditing purposes, because Requirement R1 conditions are intended to be unchanged unless the Transmission Operator is otherwise notified, the Generator Owner only needs to provide the documentation to the Transmission Operator one time, or whenever the operating specifications change.

For auditing purposes, if a PSS is in service but is not providing an active signal to the AVR as described in Requirement R1, the disabled period does not count against the Requirement R2 mandate to be in service except as otherwise allowed.

R2. Each Generator Operator shall have its PSS in service while synchronized, except during any of the following: *[Violation Risk Factor: Medium] [Time Horizon: Operating Assessment]*

- Component failure
- Testing of a Bulk Electric System Element affecting or affected by the PSS
- Maintenance
- As agreed upon by the Generator Operator and the Transmission Operator

A PSS that is out of service for less than 30 minutes does not create a violation of this Requirement, regardless of cause.

M2. Each Generator Operator will have documentation of each claimed exception specified in Requirement R2. Documentation may include, but is not limited to:

- A written explanation covering the bulleted exception that describes the circumstances of the exception as allowed in Requirement R2.
- Documented evidence that the Generator Operator and the Transmission Operator agreed the PSS would not be operating during a specified set of circumstances, where the exception is claimed under the last bullet of Requirement R2.

For auditing purposes, the presumption is that the PSS was in service unless otherwise exempted in Requirement R2. Evidence need only be provided to prove the circumstances during which the PSS was not in service for periods in excess of 30 minutes.

R3. Each Generator Owner shall tune its PSS to meet the following inter-area mode criteria, except as specified in Requirement R3, Part 3.5 below: *[Violation Risk Factor: Medium] [Time Horizon: Operating Assessment]*

3.1. PSS shall be set to provide the measured, simulated, or calculated compensated Vt/Vref frequency response of the excitation system and synchronous machine such that the phase angle will not exceed ± 30 degrees through the frequency range from 0.2 Hertz to the lesser of 1.0 Hertz or the highest frequency at which the phase of the Vt/Vref frequency response does not exceed 90 degrees.

3.2. PSS output limits shall be set to provide at least ±5% of the synchronous machine's nominal terminal voltage.

3.3. PSS gain shall be set to between 1/3 and 1/2 of maximum practical gain.

3.4. PSS washout time constant shall be no greater than 30 seconds.

3.5. Units that have an excitation system or PSS that is incapable of meeting the tuning requirements of Requirement R3 are exempt from Requirement R3 until the voltage regulator is either replaced or retrofitted such that the PSS becomes capable of meeting the tuning requirements.

M3. Each Generator Owner will have documented evidence that its PSS was tuned to meet the specifications of Requirement R3.

If the exception under Requirement R3, Part 3.5, is claimed, the Generator Owner will have documented evidence describing: 1) the conditions that render the PSS incapable of meeting the tuning requirements, and 2) the date the voltage regulator was last replaced or retrofitted.

R4. Each Generator Owner shall install and complete start-up testing of a PSS on its generator within 180 days of either of the following events: *[Violation Risk Factor: Medium] [Time Horizon: Operational Assessment]*

- The Generator Owner connects a generator to the BES, after achieving Commercial Operation, and after the Effective Date of this standard.
- The Generator Owner replaces the voltage regulator on its existing excitation system, after achieving Commercial Operation for its generator that is connected to the BES, and after the Effective Date of this standard.

M4. Each Generator Owner will have evidence that it installed and completed start-up testing of a PSS on its generator within 180 days of either of the conditions described in Requirement R4, and when those conditions occur after the Effective Date of this standard.

For auditing purposes of Requirement R4, bullet one only applies to equipment on its initial (first energization) connection to the BES.

R5. Each Generator Owner shall repair or replace a PSS within 24 months of that PSS becoming incapable of meeting the tuning specifications stated in Requirement R3. *[Violation Risk Factor: Medium] [Time Horizon: Operational Assessment]*

M5. Each Generator Owner will have evidence that it repaired or replaced its PSS within 24 months of that PSS becoming incapable of meeting the tuning specifications of Requirement R3. Evidence may include, but is not limited to, documentation of the date the PSS became incapable of meeting the Requirement R3 tuning specifications, and the date the PSS was returned to service, demonstrating that the span of time between the two events was less than 24 months.

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

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 Compliance Monitoring and Assessment Processes

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

1.3 Evidence Retention

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

Each Generator Operator shall keep evidence for all Requirements of the document for a period of three years plus calendar current.

1.4 Additional Compliance Information

None

D. Regional Differences

None

Table of Compliance Elements

R	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Planning Horizon	Low	NA	NA	NA	The Generator Owner failed to provide its PSS operating specifications to the Transmission Operator as required in Requirement R1.
R2	Operations Assessment	Medium	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 30 minutes but less than 60 minutes.	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 60 minutes but less than 120 minutes.	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 120 minutes but less than 180 minutes.	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 180 minutes.
R3	Operations Assessment	Medium	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, two times or fewer during the audit period.	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, three times during the audit period.	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, four times during the audit period.	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, five times or more during the audit period.

R	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operational Assessment	Medium	NA	NA	NA	The Generator Owner failed to install on its generator a PSS, as required in Requirement R4.
R5	Operational Assessment	Medium	NA	NA	NA	The Generator Owner failed to repair or replace a non-operational PSS as required in Requirement R5.

Version History

Version	Date	Action	Change Tracking
1	April 16, 2008	Permanent Replacement Standard for VAR-STD-002b-1	
1	October 28, 2008	Adopted by NERC Board of Trustees	
1	April 21, 2011	FERC Order issued approving VAR-501-WECC-1 (FERC approval effective June 27, 2011; Effective Date July 1, 2011)	
2	November 13, 2014	Adopted by NERC Board of Trustees	
2	March 3, 2015	FERC letter order approved VAR-501-WECC-2	
3	February 9, 2017	Adopted by NERC Board of Trustees	
3	April 28, 2017	FERC letter order approved VAR-501-WECC-3	
3.1	August 10, 2017	Adopted by the NERC Board of Trustees	Errata
3.1	September 26, 2017	FERC letter order issued approving VAR-501-WECC-3.1	
3.1	April 20,2020	The Guidelines and Technical Basis (including the Technical Rationale) section of the standard was removed and placed into a separate document. Because no changes were made to the mandatory and enforceable elements of the standard, the version number remains unchanged.	Technical Rationale Initiative

Guideline and Technical Basis

PSS systems are used to minimize real power oscillations by rapidly adjusting the field of the generator to dampen the low frequency oscillations.

It is necessary for large numbers of PSS devices to be in operation in the Western Interconnection to provide the required system damping while still allowing for some of these units to be out of service whenever necessary.

Mandate to Install a PSS

Nothing in this Regional Reliability Standard (RSS) should be construed to require installation of a PSS *solely because* a PSS is not currently installed as of the Effective Date of this RRS. Rather, installation is only mandated on the occurrence of either of the triggering events described in Requirement R4, Bullet 1 or Bullet 2, after the Effective Date of the RRS.

It should be noted that a PSS is neither Transmission nor generation.

Requirement R1

Requirement R1 addresses normal operating conditions.

Requirement R1 recognizes that PSS systems have varying states, such as on, off, active, and non-active. As long as the PSS is operating in accordance with the documentation provided to the Transmission Operator, this is not considered a status change for purposes of this standard.

This Requirement eliminates the requirement to count hours as required in the previous version of this standard while also allowing the Generator Owner to create a unit-specific operating plan.

The intent of Requirement R1 is to provide the Transmission Operator, the PSS operating zone in which the PSS is "active" providing damping to the power system. Some PSS may be programmed to become "active" at a specified megawatt loading level and above while others may be programmed to be "active" in a particular band of megawatt loading levels and are "non-active" only when passing through the "rough zone" or some other band. A "rough zone" is a megawatt loading band in which the generator-turbine system could contribute to system instability.

Requirement R2

This Requirement only applies when the PSS is out of service for a period greater than 30 minutes.

Unlike Requirement R1, Requirement R2 addresses exceptions to normal operation.

The intent of Requirement R2 is to remove the previous requirement to log hours for PSS in service. In this standard's previous version, the logged hours were totaled quarterly to meet the

~~98% in-service requirement. Instead of documenting the number of hours excluded, this Requirement simplifies the process by allowing the Generator Operator to communicate to the Transmission Operator the circumstances that render the PSS unavailable to the Transmission Operator (such as component failure, maintenance, and testing).~~

~~**Requirement R3**~~

~~Nothing in this RSS should be construed to mandate the design criteria for the *equipment* used to produce the tuning output of the PSS. Rather, Requirement R3 is intended to address the design criteria for the *tuning output* of the PSS.~~

~~Unlike the language in Requirement R5 that looks *backward* to address units that were once operating but are no longer capable of operating, Requirement R3 looks *forward*, requiring that units be tuned to the specified parameters.~~

~~The PSS transfer function should compensate the phase characteristics of the generator, exciter, and power (GEP) system transfer function so the compensated transfer function ((PSS(s) * GEP(s)) has a phase characteristic of ± 30 degrees in the frequency range.~~

~~The GEP(s) transfer function is a theoretical transfer function and its phase characteristic cannot be directly measured during field tests (only via simulation). Thus, the Requirement recognizes the practical approach of measuring the frequency response between voltage reference set point and terminal voltage (Et/Vref) and using the phase characteristic of such frequency response as being the phase characteristic of GEP(s). The phase characteristic of Et/Vref is a better approximation to the phase characteristic of GEP(s) when the frequency response Et/Vref is obtained with the generator synchronized to the grid at its minimum stable power output.~~

~~In an effort to allow for reasonable wash-out time constants, the Requirement specifies 0.2 Hz as the applicable threshold. The 0.2 Hz threshold more closely aligns with the observed oscillation frequencies.~~

~~A properly tuned PSS should provide positive damping to the local mode of oscillation, which typically has a frequency higher than 1.0 Hz.~~

~~This Requirement modifies the requirement associated with the adjustment of the PSS gain. The standard no longer defines the PSS gain in terms of gain margin but instead requires the final PSS gain to be between 1/3 (10 dB) and 1/2 (6 dB) of the maximum practical gain that could be achieved during PSS commissioning. The maximum practical gain might be associated with the excessive noise or raised higher-frequency oscillations in the closed loop response (exciter mode) or any other form if there is inadequate closed-loop performance, as determined during PSS commissioning. It is now part of Measure M3 to show the field test results that led to the determination of the maximum practical gain.~~

Requirement R4

Requirement R4 requires a Generator Owner to install a PSS on new applicable units or when excitation systems are replaced or retrofitted on existing applicable units. This Requirement applies to new excitation systems and not to existing systems that do not have PSS. The Requirement also allows a reasonable amount of time for the commissioning of new PSS.

Requirement R5

Unlike the language in Requirement R3 that looks *forward* to ensure that a unit is tuned, Requirement R5 looks *backward*. Specifically, the language in Requirement R5, "becoming incapable," indicates the unit was previously capable of meeting the tuning requirements in Requirement R3, but is no longer capable. Restated, Requirement R5 addresses units that were previously working but are now no longer working.

The intent of Requirement R5 is to remove the "tiered" approach to PSS repair/replacement following a failure. A simple, streamlined approach to allow the Generator Owner sufficient time to repair or replace a broken PSS has been written. Consideration has been given for the need to procure parts or new equipment, schedule an equipment/unit outage, and install and test the repaired or replaced PSS. It is recognized that in some instances, it may require (1) replacement of an AVR, and (2) the existence of a PSS, or both the AVR and the PSS may need to be replaced to achieve a functioning system.

The 24-month time frame is sufficient to return a functional, operating PSS to service.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard VAR-501-WECC-3 — Power System Stabilizer

United States

Standard	Requirement	Enforcement Date	Inactive Date
VAR-501-WECC-3	TBD	TBD	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard BAL-005-1

April 20, 2020

BAL-005-1 – Balancing Authority Control

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 R1: Real-time operation of a Balancing Authority requires real-time information. A sufficient scan rate is key to an Operator's trust in real-time information. Without a sufficient scan rate, an operator may question the accuracy of data during events, which would degrade the operator's ability to maintain reliability.

Rationale for Requirement R2: The RC is responsible for coordinating the reliability of bulk electric systems for member BA's. When a BA is unable to calculate its ACE for an extended period of time, this information must be communicated to the RC within 15 minutes thereafter so that the RC has sufficient knowledge of system conditions to assess any unintended reliability consequences that may occur on the wide area.

Rationale for Requirement R3: Frequency is the basic measurement for interconnection health, and a critical component for calculating Reporting ACE. Without sufficient available frequency data the BA operator will lack situational awareness and will be unable to make correct decisions when maintaining reliability.

Rationale for Requirement R4: System operators utilize Reporting ACE as a primary metric to determine operating actions or instructions. When data inputs into the ACE calculation are incorrect, the operator should be made aware through visual display. When an operator questions the validity of data, actions are delayed and the probability of adverse events occurring can increase.

Rationale for Requirement R5: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Since Reporting ACE is a measure of the BA's reliability performance for BAL-001, and BAL-002, it is critical that Reporting ACE be sufficiently available to assure reliability.

Rationale for Requirement R6: Reporting ACE is a measure of the BA's reliability performance for BAL-

001, and BAL-002. Without a process to address persistent errors in the ACE calculation, the operator can lose trust in the validity of Reporting ACE resulting in delayed or incorrect decisions regarding the reliability of the bulk electric system.

Rationale for Requirement R7: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Common source data is critical to calculating Reporting ACE that is consistent between Balancing Authorities. When data sources are not common, confusion can be created between BAs resulting in delayed or incorrect operator action.

The intent of Requirement R7 Part 7.1 is to provide accuracy in the measurement and calculations used in Reporting ACE. It specifies the need for common metering points for instantaneous values for the tie-line megawatt flow values between Balancing Authority Areas. Common data source requirements also apply to instantaneous values for pseudo-ties and dynamic schedules, and can extend to more than two Balancing Authorities that participate in allocating shares of a generation resource in supplementary regulation, for example.

The intent of Requirement R7 Part 7.2 is to enable accuracy in the measurements and calculations used in Reporting ACE. It specifies the need for common metering points for hourly accumulated values for the time synchronized tie line MWh values agreed-upon between Balancing Authority Areas. These time synchronized agreed-upon values are necessary for use in the Operating Process required in R6 to identify and mitigate errors in the scan-rate values used in Reporting ACE.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard EOP-008-2

April 20, 2020

EOP-008-2 – Loss of Control Center Functionality

Rationale

Rationale for Requirement R1: The phrase "data exchange capabilities" is replacing “data communications in Requirement R1, Part 1.2.2 for the following reasons:

COM-001-1 (no longer enforceable) covered telecommunications, which could be viewed as covering both voice and data. COM-001-2.1 (currently enforceable) focuses on "Interpersonal Communication" and does not address data.

The topic of data exchange has historically been covered in the IRO / TOP Standards. Most recently the revisions to the standards that came out of Project 2014-03 Revisions to TOP and IRO Standards use the phrase "data exchange capabilities." The rationale included in the IRO-002-4 standard discusses the need to retain the topic of data exchange, as it is not addressed in the COM standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard NUC-001-3

April 20, 2020

NUC-001-3 – Nuclear Plant Interface Coordination

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 R5:
The NUC FYRT recommended R5 be revised for consistency with R4 and to clarify that nuclear plants must be operated to meet the Nuclear Plant Interface Requirements.

Rationale for R7 and R8:
The NUC FYRT recommended deleting “Protection Systems” in Requirements R7 and R8 since it is a subset of the "nuclear plant design" and "electric system design" elements currently contained in R7 and R8 respectively; and adding a parenthetical clause (e.g. protective setpoints) to R7 following "nuclear plant design" and parenthetical clause (e.g. relay setpoints) to R8 following "electric system design."

Rationale for R9:
The NUC FYRT recommended that R9 be revised to clarify that all agreements do not have to discuss each of the elements in R9, but that the sum total of the agreements need to address the elements. In addition, for clarity in Part 9.4.1, the NUC FYRT recommended that "affecting the NPIRs" be inserted following "Provisions for communications" and "applicable unique" be inserted following ""definitions of."

Rationale for R9.3.7:
The term “Special Protection Systems” (SPS) was replaced with “Remedial Action Schemes” (RAS) in order to align with other current NERC standards development work in Project 2010-05.2: Special Protection Systems. Project 2010-05.2 has proposed to replace SPS with RAS throughout all of the NERC Standards in order to move to the use of a single term. RAS and SPS have the same definition in the NERC Glossary of Terms.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard PRC-005-6

April 20, 2020

PRC-005-6 – Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance

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 revisions to Automatic Reclosing:

To address directives from FERC Order No. 803 addressing Automatic Reclosing, the definition for Automatic Reclosing was revised to add supervisory relays, the associated voltage sensing devices, and the associated control circuitry.

Rationale for revisions to Component Type:

With the revision of the definition of Automatic Reclosing, there are four specific elements of this definition, rather than two as stated in the prior version.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard PRC-006-3

April 20, 2020

PRC-006-3 – Automatic Underfrequency Load Shedding

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 R9:

The "Corrective Action Plan" language was added in response to the FERC directive from Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a Planning Coordinator (PC) assessment. The revised language adds clarity by requiring that each UFLS entity follow the UFLS program, including any Corrective Action Plan, developed by the PC.

Also, to achieve consistency of terminology throughout this standard, the word "application" was replaced with "implementation." (See Requirements R3, R14 and R15)

Rationale for R10:

The "Corrective Action Plan" language was added in response to the FERC directive from Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a PC assessment. The revised language adds clarity by requiring that each UFLS entity follow the UFLS program, including any Corrective Action Plan, developed by the PC.

Also, to achieve consistency of terminology throughout this standard, the word "application" was replaced with "implementation." (See Requirements R3, R14 and R15)

Rationale for R15:

Requirement R15 was added in response to the directive from FERC Order No. 763, which raised concern that the standard failed to specify how soon an entity would need to implement corrections after a deficiency is identified by a PC assessment. Requirement R15 addresses the FERC directive by making explicit that if deficiencies are identified as a result of an assessment, the PC shall develop a Corrective Action Plan and schedule for implementation by the UFLS entities.

A “Corrective Action Plan” is defined in the NERC Glossary of Terms as, “a list of actions and an associated timetable for implementation to remedy a specific problem.” Thus, the Corrective Action Plan developed by the PC will identify the specific timeframe for an entity to implement corrections to remedy any deficiencies identified by the PC as a result of an assessment.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard PRC-006-SERC-02

April 20, 2020

PRC-006-SERC-02 – Automatic Underfrequency Load Shedding Requirements

Guidelines and Technical Basis

1. **Existing UFLS schemes**
   Each Planning Coordinator should consider the existing UFLS programs which are in place and should consider input from the UFLS entities in developing the UFLS scheme.

2. **Basis for SERC standard requirements**
   SERC Standard PRC-006-SERC-02 is not a stand-alone standard, but was written to be followed in conjunction with NERC Standard PRC-006-1. The primary focus of SERC Standard PRC-006-SERC-02 was to provide region-specific requirements for the implementation of the higher tier NERC standard requirements with the goals of a) adding clarity and b) providing for consistency and a coordinated UFLS scheme for the SERC Region as a whole.
   Generally speaking, requirements already in the NERC standard were not repeated in the SERC standard. Therefore, both the NERC and SERC standards must be followed to ensure full compliance.

3. **Basis for applying a percentage load shedding value to Forecast Load versus Actual Load**
   The Planning Coordinator will develop a UFLS scheme to meet the performance requirements of NERC Standard PRC-006-2 Requirement R3 and SERC Standard PRC-006- SERC-02 Requirement R2. This development will result in certain percentages of load for each UFLS entity in the Planning Coordinator's area for which automatic under frequency load shedding must be implemented. The Planning Coordinator develops these percentages based on forecast peak load demand. However, the UFLS entity implements these percentages based on the previous year's actual peak demand. Applying the same percentage to these different base values was intentional to ensure that both the Planning Coordinator and UFLS entities had a clear, measurable value to use in performing their respective roles in meeting the standard. Planning Coordinators typically use forecast demands in their work. Whereas the previous year's actual (or estimated) demand is typically more available to UFLS entities. Additionally, the use of percentages based on t h e s e different base values tends to minimize the error due to the time lag between design and actual field implementation. Since a percentage is provided by the Planning Coordinator to the UFLS entities, any differences between the design values (i.e., forecast load) and the implemented values (i.e., previous year's actual)

would naturally tend to match up reasonably well. For example, if the total planning area load in MW for which UFLS was installed during the time of implementation was slightly higher or lower than the MW value used in the design by the Planning Coordinator, multiplying by the specified percentage would result in an implemented load shedding scheme that also had a reasonably similar higher or lower MW value.

4. **Basis for May 1 and 18 month time frames**
   Each UFLS entity must annually review that the amount of UFLS load shedding implemented is within a certain tolerance as specified by SERC Standard PRC-006-SERC-02 Requirement R 4 or Requirement R5 by May 1 of the current year. May 1 was chosen to allow sufficient time after the previous year's peak occurred to make adjustments in the field to the implementation if necessary to meet the tolerances specified in Requirement R4 or Requirement R5. Therefore, the May 1 date applies only to implementation of the existing percentages of load shedding specified by the Planning Coordinator. On the other hand, the 18-month time frame specified in PRC-006-SERC-02 Requirement R6 is intended to allow sufficient budgeting, procurement, and installation time for additional equipment, or for significant setting changes to existing equipment necessary to meet a revised load shedding scheme design that has been specified by the Planning Coordinator. During this 18-month transition period, the May 1 measurement of R4 or Requirement R5 would not apply.

5. **Basis for smaller entity threshold of 100 MW**
   Most distribution substations have transformers rated in the range of 10 to 40 MVA. Usually most transformers would serve 1 to 4 feeders and each feeder will normally carry between 8 and 10 MVA. In general, assuming that each feeder would carry 10 MW, an entity with a load slightly greater than 100 MW would have at least 10 feeders available. For a program with three 10 % steps, only 3 feeders would be required to have under frequency load shed capabilities. The 100 MW threshold seems to provide adequate flexibility for implementing load shedding in three steps for entities slightly greater than 100 MW.

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 each of the rationale text boxes was moved to this section.

Rationale for R1:

Studying the Region as an island is required by the NERC standard. Most regions have only one or a few different UFLS schemes. Where there is more than one scheme, studying this island demonstrates that the schemes are coordinated and performing adequately. Because there are so many different UFLS schemes in SERC (18 different schemes were represented in the 2007 SERC UFLS study), the SDT believes that applying the schemes to each subregion as an island is a necessary additional test of the coordination of the various UFLS schemes. Without this additional test, a poorly performing scheme may be masked by the large number of good performing schemes in the Region. A subregion island study, which would have a smaller number of schemes, would be more likely to uncover the poorly performing scheme and therefore get it fixed. This approach will result in a much better overall

performance of the UFLS programs in SERC. The SDT recognized that there may be simulation problems due to opening the ties to utilities outside the subregion. Therefore, the subregion island boundaries are allowed to be adjusted to produce an island more suitable for simulation.

(Note: The SERC Subregions are identified in paragraph 4.2 of the SERC Reliability Corporation Bylaws: "The Region is currently geographically divided into five subregions that are identified as Southeastern, Central, VACAR, Delta, and Gateway.")

Rationale for R2:
These requirements for the UFLS schemes in SERC have been in place for many years (except 2.6). The SDT believes that these requirements are still needed to ensure consistency for the various schemes which are used in SERC. Part 2.6 is designed to prevent spurious operations due to transient frequency swings.

Rationale for R3:
R4 of the NERC standard PRC-006-1 requires the PC to conduct assessments of UFLS schemes through dynamic simulations to verify that they meet performance requirements for generation/load imbalances of up to 25%. This requirement defines specific imbalances that are to be studied within SERC. The 13% and 22% levels were determined from simulations of the worst case frequency overshoot for the UFLS schemes in SERC.

Rationale for R4:
The SDT believes it is necessary to put a requirement on how well the UFLS scheme is implemented. This requirement specifies how close the actual load shedding amounts must be to the percentage of load called for in the scheme. A 4 percentage point range is allowed for each individual step, but the allowed range for all steps combined is 6 percentage points.

Rationale for R5:
The SDT believes it is necessary to put a requirement on how well the UFLS scheme is implemented. This requirement specifies how close the actual load shedding amounts must be to the percentage of load called for in the scheme. The SDT recognizes that UFLS entities with a load of less than 100 MW may have difficulty in implementing more than one UFLS step and in meeting a tight tolerance. The basis of the 100 MW comes from typical feeder load dropped by UFLS relays, and the use of a 100 MW threshold in other regional UFLS standards.

Rationale for R6:
The SDT believes it is necessary to put a requirement on how quickly changes to the scheme should be implemented. This requirement specifies that changes must be implemented within 18 months of notification by the PC. The 18 month interval was chosen to give a reasonable amount of time for making changes in the field. All of the SERC Region has existing UFLS schemes which, based on periodic simulations, have provided reliable protection for years. Events which result in islanding and an activation of the UFLS schemes are extremely rare in SERC. Therefore, the SDT does not believe that changes to an existing UFLS scheme will be needed in less than 18 months. However, if a PC determines there is a need for changing the UFLS scheme faster than 18 months, then the PC may require the

implementation to be done sooner as allowed by NERC Reliability Standard PRC-006-1.

Rationale for R7:
The NERC standard requires that a UFLS database be maintained by the Planning Coordinator. This requirement specifies what data must be reported to SERC. A SERC UFLS database is needed to facilitate data sharing across the SERC Region, with other regions, and with NERC.

Rationale for R8:
The SDT believes that generator over and under frequency tripping data is needed to supplement the UFLS data provided by the Planning Coordinator for post-event analysis of frequency disturbances. This requirement states what data must be reported to SERC by the Generator Owners. Since the inverse time curve cannot easily be placed into the SERC database, four clearing times based on data from the curve are requested. These clearing times are intended to cover a range of frequencies needed for event replication as well as provide information about generators that trip at a higher frequency than is allowed by the NERC standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard TOP-002-4

April 20, 2020

TOP-002-4 – Operations Planning

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:

Terms deleted in Requirement R1 as they are now contained in the revised definition of Operational Planning Analysis.

Rationale for R2:

The change to Requirement R2 is in response to NOPR paragraph 42 and in concert with proposed changes made to proposed TOP-001-4.

Rationale for R3:

Changes in response to IERP recommendation.

Rationale for R4 and R5:

These Requirements were added to address IERP recommendations.

Rationale for R6 and R7:
Added in response to SW Outage Report recommendation 1.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard TOP-003-3

April 20, 2020

TOP-003-3 – Operational Reliability Data

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard TOP-010-1(i)

April 20, 2020

TOP-010-1(i) – Real-Time Reliability Monitoring and Analysis Capabilities

Guidelines and Technical Basis

Real-time monitoring, or monitoring the Bulk Electric System (BES) in Real-time, is a primary function of Reliability Coordinators (RCs), Transmission Operators (TOPs), and Balancing Authorities (BAs) as required by TOP and IRO Reliability Standards. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. Real-time monitoring may include the following activities performed in Real-time:

- Acquisition of operating data;
- Display of operating data as needed for visualization of system conditions;
- Audible or visual alerting when warranted by system conditions; and
- Audible or visual alerting when monitoring and analysis capabilities degrade or become unavailable.

Requirement R1

The TOP uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform monitoring and Real-time Assessments appear in other Reliability Standards.

The TOP's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R1 Part 1.1. The criteria support identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 specifies the TOP shall include actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments. Requirement R1 Part 1.3 is focused on addressing data point quality issues affecting Real-time Assessments. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R1 Part 1.3.

The TOP's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the TOP to meet its obligations for performing the Real-time Assessment. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the TOP;
- Following processes established for resolving data conflicts as specified in TOP-003-3, or other applicable Reliability Standards;
- Taking corrective actions on the TOP's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the TOP's Real-time Assessment; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the quality of the Real-time Assessment so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R2

The BA uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The BA's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R2 Part 2.1. The criteria supports identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 specifies the BA shall include in its Operating Process or Operating Procedure actions to address Real-time data quality issues when data quality affects its analysis functions. Requirement R2 Part 2.3 is focused on addressing data point quality issues affecting analysis functions. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R2 Part 2.3.

The BA's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the BA to meet its obligations for performing its analysis functions. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the BA;
- Following processes established for resolving data conflicts as specified in TOP-003-3 or other applicable Reliability Standards;
- Taking corrective actions on the BA's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the BA's analysis functions; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the analysis quality so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R3

Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments may include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

Examples of the types of criteria used to evaluate the quality of analysis used in Real-time Assessments may include solution tolerances, mismatches with Real-time data, convergences, etc.

The Operating Process or Operating Procedure must describe how the quality of analysis results used in Real-time Assessment will be shown to operating personnel.

Requirement R4

Requirement R4 addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

An alarm process monitor could be an application within a Real-time monitoring system or it could be a separate system. 'Heartbeat' or 'watchdog' monitors are examples of an alarm process monitor. An alarm

process monitor should be designed and implemented such that a stall of the Real-time monitoring alarm processor does not cause a failure of the alarm process monitor.

Rationale:

Rationale for Requirement R1: The Transmission Operator (TOP) uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform Real-time monitoring and Real-time Assessments appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 of this standard specifies the TOP shall include actions to address Real-time data quality issues affecting its Real-time Assessments in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process used to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2, provided that this process addresses Real-time data quality issues. The revision in Part 1.3 to address Real-time data quality issues *when data quality affects Real-time Assessments* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R2: The Balancing Authority (BA) uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 of this standard specifies the BA shall include actions to address Real-time data quality issues affecting its analysis functions in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2 provided that this process addresses Real-time data quality issues.

The revision in Part 2.3 to address Real-time data quality issues *when data quality affects its analysis functions* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R3: Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time

Assessments include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

The Operating Process or Operating Procedure must include provisions for how the quality of analysis results used in Real-time Assessment will be shown to operating personnel. Operating personnel includes System Operators and staff responsible for supporting Real-time operations.

Rationale for Requirement R4: The requirement addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

The requirement in Draft Two of the proposed standard has been revised for clarity by removing the term *independent*. The alarm process monitor must be able to provide notification of failure of the Real-time monitoring alarm processor. This capability could be provided by an application within a Real-time monitoring system or by a separate component used by the System Operator. The alarm process monitor must not fail with a simultaneous failure of the Real-time monitoring alarm processor.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard VAR-501-WECC-3.1

August 20, 2020

VAR-501-WECC-3.1 – Power System Stabilizer (PSS)

Guidelines and Technical Basis

PSS systems are used to minimize real power oscillations by rapidly adjusting the field of the generator to dampen the low-frequency oscillations.

It is necessary for large numbers of PSS devices to be in operation in the Western Interconnection to provide the required system damping while still allowing for some of these units to be out of service whenever necessary.

Mandate to Install a PSS

Nothing in this Regional Reliability Standard (RSS) should be construed to require installation of a PSS *solely because* a PSS is not currently installed as of the Effective Date of this RRS. Rather, installation is only mandated on the occurrence of either of the triggering events described in Requirement R4, Bullet 1 or Bullet 2, after the Effective Date of the RRS.

It should be noted that a PSS is neither Transmission nor generation.

Requirement R1

Requirement R1 addresses normal operating conditions.

Requirement R1 recognizes that PSS systems have varying states, such as on, off, active, and non-active. As long as the PSS is operating in accordance with the documentation provided to the Transmission Operator, this is not considered a status change for purposes of this standard.

This Requirement eliminates the requirement to count hours as required in the previous version of this standard while also allowing the Generator Owner to create a unit-specific operating plan.

The intent of Requirement R1 is to provide the Transmission Operator, the PSS operating zone in which the PSS is “active” providing damping to the power system. Some PSS may be programmed to become “active” at a specified megawatt loading level and above while others may be programmed to be “active” in a particular band of megawatt loading levels and are “non-active” only when passing through the

"rough zone" or some other band. A "rough zone" is a megawatt loading band in which the generator-turbine system could contribute to system instability.

Requirement R2
This Requirement only applies when the PSS is out of service for a period greater than 30 minutes.

Unlike Requirement R1, Requirement R2 addresses exceptions to normal operation.

The intent of Requirement R2 is to remove the previous requirement to log hours for PSS in service. In this standard's previous version, the logged hours were totaled quarterly to meet the 98% in-service requirement. Instead of documenting the number of hours excluded, this Requirement simplifies the process by allowing the Generator Operator to communicate to the Transmission Operator the circumstances that render the PSS unavailable to the Transmission Operator (such as component failure, maintenance, and testing).

Requirement R3
Nothing in this RSS should be construed to mandate the design criteria for the *equipment* used to produce the tuning output of the PSS. Rather, Requirement R3 is intended to address the design criteria for the *tuning output* of the PSS.

Unlike the language in Requirement R5 that looks backward to address units that were once operating but are no longer capable of operating, Requirement R3 looks *forward*, requiring that units be tuned to the specified parameters.

The PSS transfer function should compensate the phase characteristics of the generator, exciter, and power (GEP) system transfer function so the compensated transfer function ((PSS(s) * GEP(s)) has a phase characteristic of ± 30 degrees in the frequency range.

The GEP(s) transfer function is a theoretical transfer function and its phase characteristic cannot be directly measured during field tests (only via simulation). Thus, the Requirement recognizes the practical approach of measuring the frequency response between voltage reference set point and terminal voltage (Et/Vref) and using the phase characteristic of such frequency response as being the phase characteristic of GEP(s). The phase characteristic of Et/Vref is a better approximation to the phase characteristic of GEP(s) when the frequency response Et/Vref is obtained with the generator synchronized to the grid at its minimum stable power output.

In an effort to allow for reasonable wash-out time constants, the Requirement specifies 0.2 Hz as the applicable threshold. The 0.2 Hz threshold more closely aligns with the observed oscillation frequencies. A properly tuned PSS should provide positive damping to the local mode of oscillation, which typically has a frequency higher than 1.0 Hz.

This Requirement modifies the requirement associated with the adjustment of the PSS gain. The standard no longer defines the PSS gain in terms of gain margin but instead requires the final PSS gain to be

between 1/3 (10 dB) and 1/2 (6 dB) of the maximum practical gain that could be achieved during PSS commissioning. The maximum practical gain might be associated with the excessive noise or raised higher-frequency oscillations in the closed loop response (exciter mode) or any other form if there is inadequate closed-loop performance, as determined during PSS commissioning. It is now part of Measure M3 to show the field test results that led to the determination of the maximum practical gain.

Requirement R4

Requirement R4 requires a Generator Owner to install a PSS on new applicable units or when excitation systems are replaced or retrofitted on existing applicable units. This Requirement applies to new excitation systems and not to existing systems that do not have PSS. The Requirement also allows a reasonable amount of time for the commissioning of new PSS.

Rationale for R5

Unlike the language in Requirement R3 that looks *forward* to ensure that a unit is tuned, Requirement R5 looks *backward.* Specifically, the language in Requirement R5, "becoming incapable," indicates the unit was previously capable of meeting the tuning requirements in Requirement R3, but is no longer capable. Restated, Requirement R5 addresses units that were previously working but are now no longer working.

The intent of Requirement R5 is to remove the "tiered" approach to PSS repair/replacement following a failure. A simple, streamlined approach to allow the Generator Owner sufficient time to repair or replace a broken PSS has been written. Consideration has been given for the need to procure parts or new equipment, schedule an equipment/unit outage, and install and test the repaired or replaced PSS. It is recognized that in some instances, it may require (1) replacement of an AVR, and (2) the existence of a PSS, or both the AVR and the PSS may need to be replaced to achieve a functioning system.

The 24-month time frame is sufficient to return a functional, operating PSS to service.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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-032-1 Data for Power System Modeling and Analysis		
Date Submitted:	12/30/2019		
SAR Requester			
Name:	Kun Zhu (NERC SPIDERWG Chair) Bill Quaintance (NERC SPIDERWG Vice Chair)		
Organization:	Kun Zhu – MISO Bill Quaintance – Duke Energy Progress		
Telephone:	Kun – 317-249-5789 Bill – 919-546-4810	Email:	kzhu@misoenergy.org william.quaintance@duke-energy.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?):

As the penetration of distributed energy resources (DER) continues to increase across the North American bulk power system (BPS), it is necessary to account for DER in the planning, operation, and design of the BPS. The NERC System Planning Impacts of Distributed Energy Resources Working Group (SPIDERWG) has identified the need for improved modeling of aggregate DER for planning studies (including both utility-scale and retail-scale DER). MOD-032-1 addresses the gathering of modeling data to build interconnection-wide base cases for the planning horizon but the standard currently has no specific reference to DER data. This SAR proposes to update MOD-032-1 to: (1) include "data

Requested information
requirements and reporting procedures"[1] for DER that are necessary to support the development of accurate interconnection-wide models, (2) replace Load-Serving Entity (LSE) with Distribution Provider (DP) because of the removal of LSEs from the NERC registry criteria, (3) enable the SDT to review any additional gaps in DER data collection with the de-registration of LSE.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
This SAR proposes to revise MOD-032-1 to address gaps in data collection for the purposes of modeling and interconnection-wide case creation regarding DER. The goal is to provide clarity and consistency for data collection across Planning Coordinators (PCs) and Transmission Planners (TPs) when coordinating with the DP to gather aggregate load and DER data.
Project Scope (Define the parameters of the proposed project):
The proposed scope of this project is as follows: a. The table in Attachment 1 should be updated to include DER in the steady-state and dynamics columns. Details of the changes to be considered by the Standard Drafting Team are included in the "Detailed Description" below. b. Based on item a.) and the detailed description below, the SDT should consider whether including a definition for "Distributed Energy Resource (DER)" in the NERC Glossary of Terms is necessary. c. In alignment with the SAR submitted by the previous NERC Essential Reliability Services Working Group (ERSWG), LSE should be removed and replaced by DP as the applicable entity in Section 4.1.3 and all instances in the standard requirements and attachments. d. The SDT should review any potential gaps regarding data collection for aggregate DER data with the de-registration of LSE.
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[2] 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):
This SAR proposes to address the issues identified in the project scope above. Specifically, the following details should be considered and addressed by the drafting team: • In the Applicability section of MOD-032-1, LSE should be replaced with DP, in alignment with the SAR previously submitted by ERSWG. Similarly, all relevant uses of LSE should be replaced with DP.

[1] See Requirement R1 of MOD-032-1, which requires each TP and PC to develop data requirements and reporting procedures for the collection of modeling data used for the development of models for each PC footprint.
[2] 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 table in Attachment 1 should include references to aggregate DER in the steady-state and dynamics columns. The drafting team should consider the data needed for modeling aggregate DER for the purposes of BPS reliability studies. However, the NERC SPIDERWG proposes that the SDT consider including, at a minimum, the following information in the table: o Steady-State: ▪ Aggregate Distributed Energy Resources • Aggregate maximum and minimum active power capacity • Location (correlated to BPS bus location) • Breakdown by type of DER (e.g., by fuel type or technology) o Dynamics: ▪ Aggregate Distributed Energy Resources • Note that the SPIDERWG does not see a need to modify the short circuit column of Attachment 1 because #1 already states "all applicable elements" in the steady-state column should have necessary information related to positive, negative, and zero sequence data provided accordingly. If the TP/PC determines that aggregate DER is needed for these studies, then they have the capability to request such data. However, this is not a prevalent issue currently. • In alignment with adding "DER" to the Attachment 1 table regarding necessary data for modeling purposes, it may be needed (based on the discretion of the SDT) to add a definition for "Distributed Energy Resource (DER)" to the NERC Glossary of Terms. The SPIDERWG is in the process of developing recommended practices and NERC Reliability Guidelines related to data collection for DER modeling. These materials will provide detailed guidance for TPs and PCs to develop their data requirements and reporting procedures, per MOD-032-1. These materials are not intended to dilute the criticality of this SAR to address the issues identified above within MOD-032-1 itself. Rather, the SDT can use these materials as they become available when determining the specific language for inclusion in the standard requirements revisions.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impacts are not fully known. However, due to the limited scope of the requested data, cost impact is expected to be minimal to all entities. DPs typically collect the maximum capacity and location of DER connected to their systems during the interconnection process. Therefore, data collection effort by the DP would be minimal additional effort. DPs already have processes to provide load data to the TP and PC, so DER data can be managed in a similar manner to reduce cost and effort. If the scope of the required data is expanded, cost impact would likely increase.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.* Dispersed Generation Resources):
DER owners are not subject to NERC Reliability Standards. However, SPIDERWG believes the DP (a NERC Registered Entity) has the information regarding DER connected to its distribution system that is needed

Requested information
for modeling the aggregate behavior of DER for the purposes of planning studies. The DP should provide that information to the TP and PC accordingly.
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):
Transmission Planner, Planning Coordinator, Distribution Provider While not a Functional Entity per the NERC Functional Model, the "MOD-032 Designees" that are designated by the ERO to develop interconnection-wide base cases (i.e., the Regional Entities), will also be affected by these changes and should be considered for appointment to the Standard Drafting Team.
Do you know of any consensus building activities[3] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The proposals in this SAR were developed by the NERC SPIDERWG, a stakeholder group under the NERC Planning Committee.
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)?
The ERSWG submitted a SAR related to MOD-032-1, as described above. This SAR supports those changes, and further expands on a few necessary additional changes related to DER modeling.
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 NERC SPIDERWG is preparing a Reliability Guideline on data collection for DER modeling. That guideline will provide recommendations for improvements to the data requirements and reporting procedures developed jointly by PCs and their TPs. However, updates to MOD-032-1 are also needed to ensure minimum planning consideration and reporting requirement on DER, particularly in Attachment 1. Therefore, this SAR aligns with the necessary changes to meet the objective.

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] 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
None	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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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 "*Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards*".
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 "*Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards*". 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.
"*Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards*" 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
e.g. 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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Transmission Connected Dynamic Reactive Resources and HVDC Equipment – Assessment of Applicability in Reliability Standards

NERC SAMS White Paper
February 2019

Background

The bulk power system (BPS) in North America continues to experience a change in generating resources, technologies, and transmission system devices used to provide essential reliability services (ERS) such as voltage control, frequency control, and ramping/balancing capability. In particular, the BPS is experiencing a rapid change in generation resource mix, with an increasing installation base of inverter-based generation resources and accompanying retirements of synchronous generation resources. Additionally, generation is increasingly being located farther from load centers than it was in the past. These factors are contributing to an increased reliance on non-generation transmission-connected dynamic reactive resources – both rotating machine (i.e. synchronous condenser) and power-electronics based – to provide ERS in the BPS. Synchronous condensers are being used to provide dynamic reactive power and transient voltage support, as well as synchronous inertia and fault current contribution in weak grid conditions. Static var compensators (SVCs) and static compensators (STATCOMs) are increasingly being used to provide dynamic reactive power and transient voltage support.

Many relevant NERC Reliability Standards are not applicable to these types of transmission-connected dynamic reactive resources. It is now clear that an increasing number of these reactive resources are being used to provide the same ERS as generation resources to ensure reliability of the BPS. In many cases, these types of dynamic reactive resources are critical to BPS reliability because they are used to increase power transfer capability, mitigate system instability, provide grid resilience for physical and cyber attacks, and provide safety nets for severe contingencies. In this respect, ensuring their electrical capability, verification of performance, and ability to ride through grid events is no less important than for traditional generators.

The NERC Planning Committee and the NERC System Analysis and Modeling Subcommittee (SAMS) expressed concerns that the existing NERC Reliability Standards may not clearly address non-generation transmission-connected dynamic reactive resources. In response to these concerns, SAMS has developed this white paper that comprises an assessment of the applicability of relevant NERC Reliability Standards to such dynamic reactive resources and provides recommendations to address any identified reliability gap. In particular, SAMS focused on the following NERC Reliability Standards:

- **MOD-025-2:** Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability
- **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
- **MOD-032-1:** Data for Power System Modeling and Analysis
- **PRC-019-2:** Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection
- **PRC-024-2:** Generator Frequency and Voltage Protective Relay Settings

Results from this assessment and recommendations for moving forward are provided in this white paper.

Applicability Assessment

SAMS reviewed relevant NERC Reliability Standards related to the model verification, capability testing, disturbance ride through, and protection coordination aspects of generation resources to evaluate if the transmission-connected dynamic reactive resources are included within the applicability sections of these standards. The goal was to determine the reliability need/justification for including transmission-connected dynamic reactive resources as applicable Facilities within the Applicability section of these standards.

Recommended Applicability

Table 1 shows the applicability of relevant NERC Reliability Standards to dynamic reactive resources – including both generation resources and non-generation transmission connected reactive resources. The cells with green bold font show the existing applicability and the cells with red bold italicized font show the recommended applicability based on this SAMS assessment .

For the assessed non-generation reactive resources (refer to Appendix A for their descriptions), each cell includes either a Yes or N/A as the recommendation for its inclusion as Facilities in the Applicability section of the relevant Reliability Standard. The technical basis and justification for the recommended applicability is provided in the following sub-sections.

Table 1: Applicability of Relevant NERC Reliability Standards to Dynamic Reactive Resources

	MOD-025	MOD-026	MOD-027	MOD-032	PRC-019	PRC-024
Synchronous Generator	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Inverter-Based[1] Generator	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Synchronous Condenser	**Yes**	***Yes***	***N/A***	**Yes**	**Yes**	***Yes***
SVC	***Yes***	***Yes***	***N/A***	**Yes**	***Yes***	***Yes***
STATCOM	***Yes***	***Yes***	***N/A***	**Yes**	***Yes***	***Yes***
LCC HVDC	***N/A***	***N/A***	***Yes***	**Yes**	***Yes***	***Yes***
VSC HVDC	***Yes***	***Yes***	***Yes***	**Yes**	***Yes***	***Yes***

Existing applicability
SAMS recommendation

[1] Nonsynchronous generating resource

Technical Basis for Applicability

The sub-sections below describe the technical basis and justification for applicability of the relevant NERC Reliability Standard to each type of transmission-connected dynamic reactive resource listed in Table 1.

MOD-025

The purpose of MOD-025 is to ensure that accurate information on generator gross and net Real and Reactive Power capability and synchronous condenser Reactive Power capability is available for planning models used to assess Bulk Electric System (BES) reliability. The technical justification for applicability of MOD-025 recommended in Table 1 is described below:

- **SVC:** A SVC serves many of the same purposes as a synchronous condenser, particularly the injection or absorption of dynamic reactive power to support steady-state and transient voltage conditions. Similar to a synchronous condenser, an SVC has a current injection capability that translates to a reactive power capability based on terminal voltage. For this reason, a power electronics resource like a SVC connected to the BPS should be a Facility to which MOD-025 is applicable for reactive power capability verification.
- **STATCOM:** A SVC and STATCOM are very similar in terms of being power electronic resources connected to the BPS that provide steady-state and dynamic voltage support. The STATCOM and SVC differ in their reactive capability, particularly under off-nominal voltage conditions. Their controls are also different based on the types of equipment technologies used in the different devices. Again, the power electronics have a current injection capability that translates to reactive power capability based on voltage. For this reason, STATCOM should be a Facility to which MOD-025 is applicable for reactive power capability verification.
- **LCC HVDC:** A LCC HVDC circuit is predominantly used to transfer large amounts of active power across long distances (as well as other applications such as underground cables, etc.). LCC HVDC technology inherently consumes very large quantities of reactive power at the converters. AC filters located at the converter terminals to mitigate harmonics also provide reactive power and offset its consumption from the grid. However, ac filters are comprised of static shunt reactive devices with known reactive capability ratings that do not need verification. LCC HVDC does not have independent control of active and reactive power because there is no voltage source within the converters. For these reasons, LCC HVDC should ***not*** be a Facility to which MOD-025 is applicable for reactive power capability verification.
- **VSC HVDC:** VSC HVDC is different than LCC HVDC in that it has independent control of active and reactive power because of the independent voltage source within the converters. Therefore, these elements are able to operate in automatic voltage control, controlling their terminal voltage (or some other compensated voltage) to support scheduled voltages on the BPS. Therefore, VSC HVDC should be a Facility to which MOD-025 is applicable for reactive power capability verification.

MOD-026

The purpose of MOD-026 is to verify that the generator excitation control system or plant volt/var control function model (including the power system stabilizer model and the impedance compensator model) and the model parameters used in dynamic simulations accurately represent the generator excitation control system or plant volt/var control function behavior when assessing Bulk Electric System

(BES) reliability. The technical justification for applicability of MOD-026 recommended in Table 1 is described below:

- **Synchronous Condenser:** A synchronous condenser is a synchronous machine without a prime mover (freely rotating shaft) and therefore delivers/absorbs reactive power to the BPS based on its excitation. In essence, a synchronous condenser exhibits the same dynamic behavior as a synchronous generator from the perspectives of MOD-026. A synchronous condenser should be required to provide verified dynamic models as described in MOD-026.
- **SVC:** SVCs provide dynamic reactive power to the BPS to support grid voltage, voltage stability, and power transfers. These devices include elements and controls that can respond very quickly to grid conditions (during and after faults, for example). There are no (or minimal) moving parts in these devices, and the majority of the response is determined based on the settings programmed into the controls. It is important that these control settings are verified, and the dynamic response of the model matches reality. For these reasons, SVCs should be required to provide verified dynamic models as per the intent of MOD-026.
- **STATCOM:** STATCOMs use different technology than SVCs, but they also provide dynamic reactive power to the BPS and their response is determined based on the settings programmed into the controls. Therefore, similar to SVCs, STATCOMs should be required to provide verified dynamic models as per the intent of MOD-026.
- **LCC HVDC:** For the same reasons listed in MOD-025, LCC HVDC should ***not*** be a Facility to which MOD-026 is applicable.
- **VSC HVDC:** Similar to SVCs and STATCOMs, VSC HVDC Facilities also provide dynamic reactive power to the BPS and their response is determined based on the settings programmed into the controls. Therefore, VSC HVDC should be required to provide verified dynamic models as per the intent of MOD-026.

MOD-027

The purpose of MOD-027 is to verify that the turbine/governor and load control or active power/frequency control model and the model parameters, used in dynamic simulations that assess Bulk Electric System (BES) reliability, accurately represent generator unit real power response to system frequency variations. The technical justification for applicability of MOD-027 recommended in Table 1 is described below:

- **Synchronous Condenser:** A synchronous conderser is a dynamic reactive power resource and does not have the capability to provide active power to the BPS. It does not include a turbine-governor or active power-frequency control system. Therefore, MOD-027 is not applicable..
- **SVC:** It does not include a turbine-governor or active power-frequency control system. Therefore, SVC should ***not*** be a Facility to which MOD-027 is applicable.
- **STATCOM:** A STATCOM is a dynamic reactive power resource and does not have the capability to provide active power to the BPS. It does not include a turbine-governor or active power-frequency control system. Therefore, STATCOM should ***not*** be a Facility to which MOD-027 is applicable.
- **LCC HVDC:** Although LCC HVDC is *not* a dynamic reactive power resource, it has the capability to provide active power/frequency control to the BPS. Since its active power/frequency control system

response is determined based on the settings programmed into the controls, it should be required to provide verified dynamic models as per the intent of MOD-027.

- **VSC HVDC:** A VSC HVDC is a dynamic reactive power resource and also has the capability to provide active power/frequency control to the BPS. Since its active power/frequency control system response is determined based on the settings programmed into the controls, it should be required to provide verified dynamic models as per the intent of MOD-027.

MOD-032

MOD-032 has sufficiently comprehensive applicability to include transmission-connected dynamic reactive resources for the purposes of obtaining their modeling data. Therefore, SAMS does not recommend any changes to the applicability of MOD-032.

PRC-019

The purpose of PRC-019 is to verify coordination of generating unit Facility or synchronous condenser voltage regulating controls, limit functions, equipment capabilities and Protection System settings. The technical justification for applicability of PRC-019 recommended in Table 1 is described below:

- **Synchronous Condenser:** A synchronous condenser is protected with a number of protective functions and limiters, similar to a synchronous generator. If not properly coordinated, the limiters and protection elements could potentially limit the output or trip the machine below its rated capability. Therefore, PRC-019 should be applicable to synchronous condensers.
- **SVC:** Analogous to the synchronous machines, SVCs have voltage regulating controls, limiters, and protection functions. If not properly coordinated, the limiters and protection elements could potentially limit the output or trip the SVC below its rated capability. Therefore, PRC-019 should be applicable to SVCs.
- **STATCOM:** Analogous to the SVCs, STATCOMs have active and reactive voltage regulating controls, limiters, and protection functions. If not properly coordinated, the limiters and protection elements could potentially limit the output or trip the STATCOM below its rated capability. Therefore, PRC-019 should be applicable to STATCOMs.
- **LCC HVDC:** LCC HVDC does not have independent control of active and reactive power because there is no voltage source within the converters. To the extent that LCC HVDC has voltage regulating controls, limiters, and protection functions, they, they could potentially limit the LCC HVDC output below its rated capability if not properly coordinated. PRC-019 should be applicable to LCC HVDC due to its control and protection equipment abilities.
- **VSC HVDC:** VSC HVDC does have independent control of active and reactive power because they use voltage source converters. Analogous to the SVCs and STATCOMs, the VSC HVDC has voltage regulating controls, limiters, and protection functions. If not properly coordinated, the limiters and protection elements could potentially limit the VSC HVDC output below its rated capability. PRC-019 should be applicable to VSC HVDC due to its control and protection equipment abilities.

PRC-024

In the “Evaluating Protective Relay Settings” section of PRC-024 --Attachement 2 Item #2 states that the GO must “Evaluate voltage protective relay settings assuming that additional installed generating plant reactive

support equipment (such as static VAR compensators, synchronous condensers, or capacitors) is available and operating normally." However,this evaluation focuses on reactive power devices within the generating plant and does not include similar reactive power devices that are transmission connected.
The purpose of PRC-024 is to ensure Generator Owners set their generator protective relays such that generating units remain connected during defined frequency and voltage excursions. The technical justification for applicability of PRC-024 recommended in Table 1 is described below:

- **Synchronous Condenser:** Synchronous condensers, like synchronous generators, have frequency and voltage protective relays whose settings should not be within the ride through characteristics of PRC-024. Undervoltage and overvoltage protection, overspeed protection, etc., are all applied to a synchronous condenser since it is inherently a rotating electric machine without a prime mover. The synchronous condenser is expected to ride through grid voltage and frequency excursion events to provide dynamic voltage support and provide system inertia for stabilizing wide-area system frequency. Therefore, PRC-024 should be applicable to synchronous condensers.
- **SVC:** SVCs provide dynamic reactive power support during and immediately after a grid disturbance during the transient timeframes. In this respect, its purpose and functionalty is very similar to that of synchronous condensers (and synchronous generators). The SVC would be expected to ride through grid voltage and frequency excursion events to provide dynamic voltage supportsupport herefore, PRC-024 should be applicable to SVCs.
- **STATCOM:** STATCOMs provide dynamic reactive power support during and immediately after a grid disturbance during the transient timeframes. In this respect, its purpose and functionalty is very similar to that of synchronous condensers and SVCs. The STATCOM would be expected to ride through grid voltage and frequency excursion events to provide dynamic voltage support. PRC-024 should be applicable to STATCOM.
- **LCC HVDC:** The LCC HVDC would be expected to ride through grid voltage and frequency excursion events to provide continuity of service (i.e. maintaining MW output). Therefore, PRC-024 should not be applicable to LCC HVDC.
- **VSC HVDC:** VSC HVDC provide dynamic reactive power support during and immediately after a grid disturbance during the transient timeframes. In this respect, its purpose and functionalty is very similar to that of SVCs and STATCOMs. The VSC HVDC would be expected to ride through grid voltage and frequency excursion events to provide dynamic voltage support. Therefore, PRC-024 should be applicable to VSC HVDC.

Other Considerations

The following additional considerations were noted during the assessment. While not necessarily directly related to the assessment of applicability of elements to relevant NERC Standards, SAMS believes these additional topics are important and should be addressed.

1. Definitions for the following terms should be reviewed for potential additions and/or revisions in the NERC Glossary of Terms include, but are not limited to, the following:
    a. Generator (or Generating Facility)
    b. Generating Unit Capability[2]
    c. Dynamic Reactive Power
    d. Synchronous Condenser
    e. Static Var Compensator (SVC)
    f. Static Synchronous Compensator (STATCOM)
    g. High Voltage DC (HVDC)
    h. Line Commutated Converter (LCC) HVDC
    i. Voltage Source Converter (VSC) HVDC
    j. Flexible AC Transmission Systems (FACTS)
2. NERC SAMS and the NERC Power Plant Modeling and Verification Task Force (PPMVTF) have both identified a significant inconsistency between the intent of MOD-025-2 to "ensure that accurate information on generator…capability[3] is available for planning models used to assess Bulk Electric System (BES) reliability" and the actual results obtained during testing. MOD-025-2 does not require the full (maximum achievable) reactive capability of the resource to be reached via test. This is warranted because the testing conditions likely will limit the resource from reaching its full (maximum achievable) reactive capability before other limits are reached such as system voltage, generator terminal voltage, or auxiliary bus voltage limits. While this is reasonable for testing, the standard does not require calculations to be performed to prove that the resource could reach its full (maximum achievable) reactive capability under more favorable operating conditions (i.e. when that full reactive capability is needed for maintaining voltage schedule). Therefore, there is a significant misconception in the industry that the testing results should be used as the same data submitted for MOD-032-1 for capability of the machine. This misconception is likely leading to incorrect data being supplied for the purposes of MOD-032-1 and is driven by the requirements in MOD-025-2.

[2] This is a defined term; however, the definition is not sufficiently reflective of the term.
[3] and synchronous condenser reactive power capability

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 form 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 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):
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 activities[2] 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 ☐ 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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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 standards to address Cyber Security 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 ☒ 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 project will address a directive issued by the Federal Energy Regulatory Commission (FERC) in Order No. 866 to develop modifications to the CIP Reliability Standards to require protections regarding the availability of communications links and data communicated between the bulk electric system 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.			
Project Scope (Define the parameters of the proposed project):			
This project will address the directive in Order No. 866.			

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 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):
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):
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 activities[2] 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 and Project 2019-02 BES Cyber Systems Information Access Management 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.

[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.

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 ☐ 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%			
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%			

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
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%			
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%			

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
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%			
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%			

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
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	Prokect 2006-04 - Backup Facilities - Revision 1_rc	Recirculation Ballot	7/16/2010	7/26/2010	Quorum: 93.43% Approval: 85.22%			
135	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	7/23/2010	8/2/2010	Quorum: 94.70% Approval: 58.61%			
136	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	7/24/2010	8/3/2010	Quorum: 92.99% Approval: 49.61%			
137	Project 2006-08	Project 2006-08 - Reliability Coordination - Transmission Loading Relief_rc	Recirculation Ballot	8/20/2010	8/30/2010	Quorum: 88.26% Approval: 93.93%			
138	Project 2007-04	Project 2007-04 - Certifying System Operators: PER-003-1	Initial Ballot	9/14/2010	9/24/2010	Quorum: 92.73% Approval: 79.17%			
139	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3	Initial Ballot	9/17/2010	9/27/2010	Quorum: 96.46% Approval: 21.77%			
140	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	9/24/2010	10/4/2010	Quorum: 85.71% Approval: 81.72%			
141	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	10/2/2010	10/14/2010	Quorum: 84.11% Approval: 84.52%			
142	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 3_rc	Recirculation Ballot	10/4/2010	10/14/2010	Quorum: 88.11% Approval: 99.14%			
143	Project 2009-28	Project 2009-28 - Interpretation - EOP-001-1 and EOP-001-2 for FMPP_rc	Recirculation Ballot	10/5/2010	10/15/2010	Quorum: 92.19% Approval: 94.78%			
144	Project 2009-27	Project 2009-27 - Interpretation - TOP-002-2a for FMPAA_rc	Recirculation Ballot	10/6/2010	10/16/2010	Quorum: 91.21% Approval: 93.44%			
145	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Recirculation Ballot	10/18/2010	10/28/2010	Quorum: 89.84% Approval: 84.67%			
146	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 93.66% Approval: 43.33%			
147	Project 2010-10	Project 2010-10 FAC-013-2 Planning Transfer Capability_in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 88.54% Approval: 39.85%			
148	2010 SPM	2010 Standard Processes Manual (Proposed Changes)_in	Initial Ballot	10/28/2010	11/7/2010	Quorum: 81.61% Approval: 93.72%			

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
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		
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		

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
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		
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		

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
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%			
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%			

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
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		
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%			

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
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		
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%			

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
334	Project 2007-09	Project 2007-09_Generator Verification: PRC-024-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 75.40% Approval: 52.72%			
335	Project 2007-09	Project 2007-09_Generator Verification: MOD-025-2	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 77.94% Approval: 64.24%			
336	Project 2007-09	Project 2007-09_Generator Verification: MOD-027-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.06% Approval: 68.93%			
337	Project 2007-09	Project 2007-09_Generator Verification: PRC-019-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.51% Approval: 63.63%			
338	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 78.59%	Support 10/4/12		
339	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 92.75%	Support 10/4/12		
340	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 89.73%	Support 10/4/12		
341	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 93.73%	Support 10/4/12		
342	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.53%	Support 10/4/12		
343	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 91.79%	Support 10/4/12		
344	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.47%	Support 10/4/12		
345	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 94.60%	Support 10/4/12		
346	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 88.99%	Support 10/4/12		
347	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.67%	Support 10/4/12		
348	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation Plan	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 94.91%	Support 10/4/12		
349	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 93.23%	Support 10/4/12		
350	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Recirculation Ballot	10/24/2012	11/5/2012	Quorum: 85.14% Approval: 71.39%			
351	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	10/24/2012	11/5/2012	Quorum: 78.93% Approval: 71.04%			
352	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Successive Ballot	10/26/2012	11/6/2012	Quorum: 82.04% Approval: 76.08%	Support 11/5/12		
353	Project 2010-11	Project 2010-11 TPL footnote b Initial Ballot October 2012_in	Initial Ballot	11/9/2012	11/19/2012	Quorum: 80.45% Approval: 56.18%			
354	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Initial Ballot	11/26/2012	12/5/2012	Quorum: 84.81% Approval: 72.57%	Oppose 12/5/12		
355	Project 2013-02	Project 2013-02 - Paragraph 81	Initial Ballot	11/30/2012	12/10/2012	Quorum: 75.77% Approval: 96.45%	Support 12/10/12		
356	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Successive Ballot	12/4/2012	12/13/2012	Quorum: 76.78% Approval: 53.57%	No Consensus 12/13/12		
357	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	12/4/2012	12/13/2012	Quorum: 77.22% Approval: 57.91%			
358	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Successive Ballot	12/7/2012	12/17/2012	Quorum: 76.47% Approval: 33.23%	Oppose 12/17/12		
359	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Non-binding Poll	12/7/2012	12/17/2012	Quorum: 75.58% Approval: 34.80%			
360	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Initial Ballot	12/11/2012	12/20/2012	Quorum: 84.50% Approval: 95.60%	Support 12/19/12		
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		

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
371	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-012-1	Non-binding Poll	1/4/2013	1/14/2013	Quorum: 82.23% Approval: 24.27%			
372	Project 2013-02	Project 2013-02 - Paragraph 81	Recirculation Ballot	1/8/2013	1/17/2013	Quorum: 84.60% Approval: 95.22%	Support 12/10/12		
373	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Recirculation Ballot	1/14/2013	1/23/2013	Quorum: 87.13% Approval: 99.09%	Support 12/19/12		
374	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Recirculation Ballot	1/18/2013	1/28/2013	Quorum: 85.90% Approval: 85.57%	Support 12/19/12		
375	Project 2010-11	Project 2010-11 Recirculation Ballot Jan 2013 in	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 88.55% Approval: 69.63%	No Consensus 1/11/13		
376	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 85.67% Approval: 77.61%	Oppose 12/5/12		
377	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Successive Ballot	2/11/2013	2/20/2013	Quorum: 77.62% Approval: 50.66%	Support 9/5/12		
378	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Non-binding Poll	2/11/2013	2/20/2013	Quorum: 75.38% Approval: 50.60%			
379	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Successive Ballot	2/15/2013	2/28/2013	Quorum: 78.80% Approval: 89.01%	Support 1/11/13		
380	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Non-binding Poll	2/15/2013	2/28/2013	Quorum: 76.38% Approval: 84.24%			
381	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Initial Ballot	3/1/2013	3/11/2013	Quorum: 76.36% Approval: 54.65%			
382	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Successive Ballot	3/13/2013	3/22/2013	Quorum: 77.48% Approval: 84.27%	No Consensus 3/22/13		NPCC to abstain - international nature of the ERO and BPS is not used in Reliability Standards
383	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.58% Approval: 97.18%	Support 3/14/13		
384	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.52% Approval: 98.89%	Support 3/14/13		
385	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Recirculation Ballot	3/18/2013	3/27/2013	Quorum: 81.33% Approval: 89.44%	Support 1/11/13		
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%			

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
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
391	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
392	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-002-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
393	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-013-1	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
394	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Recirculation Ballot	4/18/2013	4/29/2013	Quorum: 80.70% Approval: 88.15%	No Consensus 3/22/13		
395	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Successive ballot	5/15/2013	5/24/2013	Quorum: 81.25% Approval: 69.23%	Support 5/23/13		The Regional Standard Committee has not expressed any concerns of significance that would warrant a ballot to reject, therefore the RSC recommends a yes vote, "Affirmative", to accept the standard
396	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Non-binding Poll	5/15/2013	5/24/2013	Quorum: 80.17% Approval: 61.11%			
397	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Successive Ballot	6/24/2013	7/3/2013	Quorum: 77.65% Approval: 52.71%			
398	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Non-binding Poll	6/24/2013	7/3/2013	Quorum: 77.12% Approval: 52.48%			
399	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Initial Ballot	7/3/2013	7/12/2013	Quorum: 85.53% Approval: 49.73%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
400	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Successive Ballot	7/10/2013	7/19/2013	Quorum: 76.32% Approval: 58.36%	No Consensus 7/19/13 [Due to the concerns expressed over the potential actions by the NERC BOT and FERC as well as the incremental improvement of the standard over the previous versions, NPCC as the Regional Entity will support the standard and submit comments.]		[illegible] organizations support the standard as written however some members expressed concern that in order to measure compliance with R1 and R2, the standard will require all Reliability Directives to be investigated to determine if RC approved and documented communication protocols have been violated. Also it was identified that TO, BA communication protocols would have to approved by the RC potentially causing some legal issues if protocols aren't approved and casts question on the enforcement of those protocols. NPCC will be submitting some helpful comments should the standard pass and some non-substantive revision be performed prior to the "final" (previously named recirculation) ballot.
401	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 76.20% Approval: 55.37%			
402	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Successive Ballot	7/10/2013	7/19/2013	Quorum: 85.05% Approval: 72.43%	Support 7/19/13		
403	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 82.51% Approval: 64.59%			
404	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Final Ballot	7/16/2013	7/25/2013	Quorum: 92.31% Approval: 74.54%	No Consensus 7/22/13		The RSC has not reached a full consensus however the majority are in support. Issues outstanding for those not in support are concern over "hitting limits" more frequently and potential issues with BA's potentially "dragging" on the interconnection. NPCC will be voting affirmative on the standard.
405	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023-3	Initial Ballot	7/26/2013	8/5/2013	Quorum: 80.05% Approval: 93.00%	Support 8/5/13		
408	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025-1	Final Ballot	8/2/2013	8/12/2013	Quorum: 89.13% Approval: 76.52%	Support 8/12/13		
406	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Initial Ballot	8/2/2013	8/12/2013	Quorum: 76.32% Approval: 62.74%	Support 8/9/13		
407	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Non-binding Poll	8/2/2013	8/12/2013	Quorum: 75.89% Approval: 55.45%			
409	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Initial Ballot	8/14/2013	8/23/2013	Quorum: 78.33% Approval: 79.42%	Support 8/23/13		
410	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Non-binding Poll	8/14/2013	8/23/2013	Quorum: 77.45% Approval: 81.37%			
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%			

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
413	Project 2010-01	Project 2010-01 - Training - PER-005-2	Ballot	8/23/2013	9/3/2013	Quorum: 75.25% Approval: 34.46%	No Consensus 8/31/13		NPCC to support with comments The most contentious issues raised by RSC members was surrounding the Control Center definition and the potential to vastly expand those needing training subject to the standard and compliance and that there was no need for a standard, rather, the FERC Directives should be addressed through other means.
414	Project 2010-01	Project 2010-01 - Training - PER-005-2	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 80.45% Approval: 34.24%			
415	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Ballot	8/23/2013	9/3/2013	Quorum: 81.89% Approval: 43.79%	Oppose 8/31/13		The standard, in the view of the group, has extensive issues including but not limited to, applicability issues, lacks clarity, missing measures, quality, and other substantive issues. NPCC will be submitting detailed comments to address these issues. The RSC does not believe it would be beneficial to support the standard at this point as the next step, if it fails the initial ballot, would still require an additional ballot prior to moving to recirculation due to the substantive changes that are needed for the next revision. NPCC will be submitting helpful comments to NERC and supporting the drafting team effort.
416	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 79.95% Approval: 44.23%			
417	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Ballot	8/26/2013	9/4/2013	Quorum: 82.29% Approval: 41.24%	Support 8/31/13		
418	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 79.66% Approval: 40.00%			
419	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Ballot	8/26/2013	9/4/2013	Quorum: 81.96% Approval: 55.76%	Support 8/31/13		
420	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 80.35% Approval: 58.97%			
421	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Additional Ballot	8/26/2013	9/4/2013	Quorum: 78.68% Approval: 66.11%	Support 8/31/13		
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%			

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
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	
448	Project 2007-11	Project 2007-11 Disturbance Monitoring - PRC-002-2	Initial Ballot	12/6/2013	12/16/2013	Quorum: 82.25% Approval: 43.29%	No Consensus 12/15/13	Affirmative	Highlights of comments received expressed: • Agreement with the methodology to determine BES locations for which data had to be captured • Use of the term "locations" • DDR for Flowgates, IROLs • Clarification needed for some data that is to be captured • Editorial suggestions
449	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1	Final Ballot	12/6/2013	12/16/2013	Quorum: 87.53% Approval: 77.49%	Support 8/31/13	Affirmative	
450	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-006-4	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 80.77%	Support 11/5/13	Affirmative	
451	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-009-2	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 72.86%	Support 11/5/13	Affirmative	
452	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-011-1	Final Ballot	12/10/2013	12/20/2013	Quorum: 84.78% Approval: 72.91%	Support 11/5/13	Affirmative	
453	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Final Ballot	12/11/2013	12/20/2013	Quorum: 87.16% Approval: 86.40%	No Consensus 8/26/13	Affirmative	
454	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4	Final Ballot	12/13/2013	12/23/2013	Quorum: 84.34% Approval: 75.35%		Affirmative	
455	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-027-1	Additional Ballot	12/9/2013	12/31/2013	Quorum: 76.60% Approval: 65.71%	No Consensus 12/27/13	Affirmative	
456	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Additional Ballot	1/10/2014	1/21/2014	Quorum: 76.92% Approval: 81.41%	Support 8/31/13	Affirmative	
457	Project 2010-01	Project 2010-01 - Training - PER-005-2	Additional Ballot	1/8/2014	1/22/2014	Quorum: 7912% Approval: 74.63%	Support 11/11/13	Affirmative	
458	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Additional Ballot	1/10/2014	1/22/2014	Quorum: 75.22% Approval: 81.19%	Support 11/5/13	Affirmative	

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	
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		
478	Project 2010-13.3	Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings	Initial Ballot	5/30/2014	6/9/2014	Quorum: 79.06% Approval: 17.02%	Does not Support--6/6/14	Negative		
475	Project 2010-02	Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Final Ballot	6/12/2014	6/23/2014	Quorum: Approval: 89.03%/83.46%	Support	Affirmative		
479	Project 2007-11	Project 2007-11 - Disturbance Monitoring - PRC-002-2	Additional Ballot	6/13/2014	6/23/2014	Quorum: 77.69% Approval: 52.29%	Support	Affirmative	Extended to achieve a quorum.	Last RSC Meeting
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 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			

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
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	Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3	Additional Ballot	9/3/2014	9/12/2014	Quorum: 84.33% Approval: 76.03%	Support--9/4/14	Affirmative	
492	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	Additional Ballot	9/10/2014	9/19/2014	Quorum: 85.75%/84.96%/84.96%/85.22%/84.96%/85.22%/85.49%/85.22%/86.28%/83.11%/83.91% Approval: 76.12%/74.23%/75.67%/85.49%/75.96%/78.67%/48.73%/78.87%/87.03%/93.34%/90.13%	TOP-001-3: Negative TOP-002-4: Affirmative TOP-003-3: Affirmative IRO-001-4: No consensus however the majority indicated an Affirmative vote IRO-002-4: Negative IRO-008-2: No consensus, a majority indicated a Negative and the others indicated abstention IRO-010-2: Affirmative IRO-014-3: Negative IRO-017-1: Affirmative Implementation Plan and Definitions: Affirmative 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% Approval: 46.73%	Negative--10/1/14		
494	Project 2010-13.3	Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings	Additional Ballot	9/26/2014	10/6/2014	Quorum: 79.01% Approval: 53.02%	Affirmative--10/1/14		
495	Project 2012-13	Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	Additional Ballot	9/29/2014	10/8/2014	Quorum: 83.24%/84.82% Approval: 80.69%/84.05%	Affirmative--10/7/14	Affirmative	
496	Project 2012-13	Project 2013-03 Geomagnetic Disturbance Mitigation	Additional Ballot	10/1/2014	10/10/2014	Quorum: 82.93% Approval: 57.95%	Affirmative--10/7/14		
497	Project 2010-05.2	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)	Additional Ballot	10/3/2014	10/14/2014	Quorum: 80.54% Approval: 75.79% Approval:	Affirmative--10/7/14		
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 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%	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
						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		
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%87.56%86.59% Approval: 83.84%/95.34%/86.00%/95.35%91.17%/83.88%/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		

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
522	Project 2014-01	2014-01 - Standards Applicability for Dispersed Generation Resources - PRC-001-1.1(ii), 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		
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%/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%	Affirmative--9/11/15		

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: 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%/97.48% 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% Approval: 96.73%	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	Quorum: 85.57% Approval: 87.36%	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% Approval: 48.10%	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	Quorum: 84.28% Approval: 74.61%	Affirmative--8/17/15		
543	Project 2010-05.3	Project 2007-06 System Protection Coordination	Final Ballot	10/5/2015	10/14/2015	Quorum: 89.16% Approval: 80.94%	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	Quorum: 89.60% Approval: 90.01%	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: 90.00% Approval: 96.38%	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	Quorum: 84.59%/84.49% Approval: 47.38%/48.00%	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% Approval: 98.17%	Affirmative--11/5/15		
548	Project 2015-07	Project 2015-07 Internal Communications Capabilities	Initial Ballot	11/6/2015	11/16/2015	Quorum: 88.18% Approval: 53.60%	Affirmative--11/13/15		
549	Project 2007-06.2	Project 2007-06.2 Phase 2 of System Protection Coordination	Additional Ballot	11/10/2015	11/19/2015	Quorum: 83.18% Approval: 57.29%	Affirmative--11/18/15		
550	Project 2010-07.1	Project 2010-07.1 Vegetation Management	Initial Ballot	12/7/2015	12/16/2015	Quorum: 85.38% Approval: 82.56%	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: 88.65% Approval: 98.26%	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	Quorum: 83.39%/80.88% Approval: 60.39%/92.94%	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: 84.13%/83.17%/84.44% Approval: 70.64%/75.54%/94.30%	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	Quorum: 82.88%/82.18% Approval: 72.13%/68.01%	Affirmative--1/25/16		

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
554	Project 2010-07.1	Project 2010-07.1 Vegetation Management	Final Ballot	1/29/2016	2/8/2016	Quorum:90.03% Approval: 96.18%	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	Quorum: 86.35%/86.98%/86.67 % Approval: 72.06%/94.61%/80.15 %	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: 88.36%/87.79% Approval: 75.68%/73.87%	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	Quorum: 75.55% Approval: 78.87%	Affirmative--3/10/16		
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		

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
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% 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% Approval: 10.36%	Abstain--3/2/17		
574	Project 2015-08	Project 2015-08 Emergency Operations EOP-004-4	Final Ballot	1/24/2017	2/2/2017	Quorum: 84.46% Approval: 93.80%	Affirmative--1/4/17		
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% Approval: 78.55%/86.00%/85.81%/85.54%	Affirmative--1/23/17		
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% Approval: 89.84%/82.92%/88.64%	Affirmative--6/8/17		
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% Approval: 88.79%/81.40%/84.19%	Affirmative--6/8/17		
579	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-2	Initial Ballot	8/2/2017	8/11/2017	Quorum: 79.87% Approval: 72.67%	Affirmative--8/3/17		
580	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Initial Ballot	8/29/2017	9/8/2017	Quorum: 80.45% Approval: 78.79%	Affirmative--9/1/17		
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% Approval: 42.74%	Affirmative--9/1/17		
582	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Initial Ballot	9/8/2017	10/23/2017	Quorum: 82.71% Approval: 30.50%	Abstain--10/18/17		
583	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-2	Final Ballot	10/20/2017	10/30/2017	Quorum: 88.74% Approval: 73.35%	Affirmative--8/3/17		
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% Approval: 66.78%	Affirmative--10/30/17		
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 Approval: 58.12%/63.17%/56.55%/76.40%/68.59%	Affirmative--11/10/17		
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% Approval: 63.91%	Affirmative--12/4/17		
587	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Additional Ballot	10/30/2017	12/13/2017	Quorum: 81.73% Approval: 88.25%	Affirmative--12/4/17		
588	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Final Ballot	1/9/2018	1/18/2018	Quorum: 82.69% Approval: 89.46%	Affirmative--12/4/17		
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% Approval: 97.50%/98.91%	Affirmative--3/2/18		
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		

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: 96.64%/97.88%	~~Affirmative--5/2/18~~		
591	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Additional Ballot	2/23/2018	4/23/2018	Quorum: 80% Approval: 26.44%	Affirmative--4/16/18		
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% Approval: 93.31%	Affirmative--4/25/18		
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% Approval: 83.71%	Affirmative--4/25/18		
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% Approval: 46.71%/37.98%	Negative--4/25/18		
595	Project 2017-06	Project 2017-06 Modifications to BAL-002-2	Initial Ballot	4/27/2018	5/8/2018	Quorum: 81.82% Approval: 80%	Abstain--5/7/17		
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		

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
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		
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%/90.13%/89.84%/90.06%/90.03%/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%/95.41%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%	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
						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%/99.38%/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		
624	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%/80.93%/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		

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
13.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR Standards		3/4/11	4/4/11	Yes 4/4/11
14.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		3/9/11	4/8/11	Yes 4/8/11
15.	RFC RoP	Notice of Proposed Changes to RFC Rules of Procedure and Request for Comments			3/1/11	4/15/11	
16.	NERC RoP	Proposed Amendments to NERC Rules of Procedure Appendices 3B and 3D	Appendices 3B and 3D		3/1/11	4/15/11	Yes 4/15/11
17.	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3 - CIP-005	CIP-005		3/29/11	4/28/11	Yes 4/27/11
18.	Project 2009-06	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	FAC-008-3		3/17/11	5/2/11	Yes 5/2/11
19.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		4/13/11	5/12/11	Yes 5/9/11
20.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		4/28/11	5/27/11	Yes 5/27/11
21.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	TPL-001-2		4/18/11	5/31/11	Yes 5/31/11
22.	Project 2007-03	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	TOP-001 through TOP-008 and PER-001		4/26/11	6/9/11	Yes 6/9/11
23.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		5/11/11	6/10/11	Yes 6/10/11
24.	NERC RoP	Rules of Procedure Development Team: BES Definition Exception Process	BES Definition Exception Process		5/11/11	6/10/11	Yes 6/10/11

RSC Meeting #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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	Yes 9/6/11
36.	N/A	DRAFT CANs Posted for Comment and Retirement of CAN-0001 through 0004	CAN-0001 through 0004 Retirement		8/31/11	9/21/11	
37.	NERC RSDP	NERC 2012-2014 Reliability Standards Development Plan	2012-2014 RSDP		9/12/11	9/26/11	Yes 9/26/11
38.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		8/15/11	9/28/11	Yes 9/28/11
39.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	BES Definition		8/26/11	10/10/11	Yes 10/10/11
40.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Technical Principles for Demonstrating BES Exceptions	Technical Principles for Demonstrating BES Exceptions		8/26/11	10/10/11	Yes 10/10/11
41.	N/A	New CAN Template, five DRAFT CANs for Industry review and CANs Status posted to NERC Compliance's Web site.	CANs		9/23/11	10/14/11	Yes 10/14/11
42.	RoP	Proposed Changes to NERC Rules of Procedure and All Appendices			9/2/11	10/17/11	
43.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Rules of procedure Modifications to Support BES Exception Requests	RoP Section 509, Section 1703 and Appendix 5C		9/13/11	10/27/11	Yes 10/27/11
44.	N/A	CAN-0010-- Definition of "Annual" and Implementation of Annual Requirements	CAN-0010 Definition of Annual		10/10/11	10/31/11	Yes 10/31/11

RSC Meeting #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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	Yes 6/20/12
90.	N/A	Adequate Level of Reliability Revised Definition and Associated Documents	Adequate Level of Reliability (ALR)		4/25/12	6/25/12	Yes 6/25/12
91.	N/A	Order 754 - Request for Data or Information	Data Request		5/11/12	6/25/12	Yes 6/25/12
92.	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Interpretation of VAR -002		5/22/12	6/27/12	Yes 6/27/12
93.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		5/29/12	6/27/12	Yes 6/27/12
94.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserve	BAL-001-1		6/4/12	7/3/12	Yes 7/3/12
			BAL-002-2		6/4/12	7/3/12	Yes 7/3/12
			BAL-012-1		6/4/12	7/3/12	Yes 7/3/12
			BAL-013-1		6/4/12	7/3/12	Yes 7/3/12
95.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		5/21/12	7/5/12	Yes 7/5/12
96.	N/A	Cost Effective Analysis Process (CEAP) for NERC ERO Standards	CEAP		5/7/12	7/6/12	Yes 7/6/12
97.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002 and IRO-001-3	COM-001, COM-002 and IRO-001-3		6/7/12	7/6/12	Yes 7/6/12
98.	Project 2006-02	Project 2006-02 – Assess Transmission Future Needs and Develop Transmission Plans	TPL-002-1b, footnote ‘b’ and TPL-001-3, footnote 12		6/19/12	7/9/12	Yes 7/9/12

RSC Meeting #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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
			RSAW		9/11/12	10/10/12	Yes 10/10/12
118.	MRO SPM	Regional Reliability Standards - MRO Standards Process Manual			8/28/12	10/11/12	
119.	N/A	Standard Process Manual Revisions to Implement SPIG Recommendations	SPIG Reco		8/29/12	10/12/12	Yes 10/10/12
120.		Revisions to Outstanding VRFs and VSLs			9/5/12	10/19/12	
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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
150.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays)	Draft SAR	Informal	4/5/13	5/6/13	Yes 5/6/13
			PRC-005-3	Formal	4/5/13	5/6/13	Yes 5/613
151.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation	PRC-023-3 PRC-025-1	Formal	4/25/13	5/24/13	Yes 5/24/13
152.	Project 2007-11	Project 2007-11 - Disturbance Monitoring — PRC-002 and PRC-018	SAR	Informal	5/03/13	6/03/13	Yes 6/3/13
153.	Project 2007-11	Project 2007-11 - Disturbance Monitoring PRC-002 and PRC-018	Request for Information	Informal	6/05/13	7/05/13	
154.	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	PRC-001 and PRC-027		6/04/13	7/03/13	Yes 7/03/13
155.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	BES Definition		5/29/13	7/12/13	Yes 7/12/13
156.	TRE Regional Standard	Regional Reliability Standard - BAL-001-TRE-01	BAL-001-TRE-01		5/31/13	7/15/13	
157.	N/A	NPCC Regional Standards Process Manual	NPCC RSPM		6/06/13	7/22/13	
158.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	COM-003-1		6/20/13	7/19/13	Yes 7/19/13
159.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	PRC-025-1		6/20/13	7/19/13	Yes 7/19/13
160.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023	PRC-023-3	Formal	6/20/13	8/05/13	Yes 8/5/13
161.	N/A	SPP RE Regional Standards Process Manual	SPP RSPM		6/26/13	8/09/13	
162.	Project 2013-03	Project 2013-03 - Geomagnetic Disturbance Mitigation	EOP-010-1	Formal	6/27/13	8/12/13	Yes 8/12/13

RSC Meeting #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
163.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005	PRC-005-3	Formal	7/10/13	8/23/13	Yes 8/23/13
164.	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards	INT-004-3 INT-006-4 INT-009-2 INT-010-2 INT-011-1	Informal	7/25/13	8/23/13	Yes 8/23/13
165.	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	MOD-001-2	Formal	7/11/13	8/26/13	Yes 8/26/13
166.	Project 2010-01	Project 2010-01 - Training - PER-005-2	PER-005-2	Formal	7/19/13	9/03/13	Yes 9/3/13
167.	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	VAR-001-4 VAR-002-3	Formal	7/19/13	9/03/13	Yes 9/3/13
168	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	MOD-032-1 MOD-033-1	Formal	7/22/13	9/04/13	Yes 9/4/13
169.	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	7/22/13	9/04/13	Yes 9/4/13
170	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System – Phase 2	BES Definition Phase 2	Formal	8/6/13	9/4/13	Yes 9/4/13
171	Project 2012-13	Project 2012-13 - NUC Five-Year Review	NUC-001-2	5-year review	7/26/13	9/9/13	Yes 9/9/13
172	2014-2016 RSDP	2014-2016 Reliability Standards Development Plan	Reliability Standards Development Plan	Annual Review	8/30/13	9/13/13	Yes 9/13/13
173	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-001-1 FAC-002-1	5-year review	8/1/13	9/16/13	Yes 9/16/13
174	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-003-3 FAC-008-3 FAC-010-2.1 FAC-011-2 FAC-013-2 FAC-014-2	5-year review	8/1/13	9/16/13	Yes 9/16/13

RSC Meeting #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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	Yes 12/5/13
189	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves	BAL-002-2	Formal	10/28/13	12/11/13	Yes 12/11/13
190	Project 2007-11	Project 2007-11 - Disturbance Monitoring	PRC-002-2	Formal	11/01/13	12/16/13	Yes 12/16/13
191	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-027	Formal	11/04/13	12/18/13	Yes 12/18/13
192	Project 2014-01	Project 2014-01 - Standards Applicability for Dispersed Generation Resources	SAR	Formal	11/20/13	12/19/13	Yes 12/19/13
193	Project 2010-01	Project 2010-01 Training - PER-005-2	PER-005-2	Formal	12/4/13	1/22/14	Yes 1/17/14
194	Project 2010-03	Project 2010-03 Modeling Date - MOD B	MOD-033-1	Formal	12/6/13	1/22/14	Yes 1/21/14
195	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	INT-004-3 INT-010-2	Formal	1/10/14	1/24/14	Yes 1/22/14
196	Project 2007-02	Project 2007-02 Operating Personnel	COM-002-4	Formal	1/22/14	1/31/14	Yes 1/31/14
197	Project 2014-02	Project 2014-02 Standard Authorization Request – Cyber Security Standards	CIP SAR	Informal	1/17/14	2/18/14	Yes 2/18/14
198	2014 Work Plan	2014 Work Plan for NERC Reliability Standards Development	2014 Work plan			2/21/13	Yes 2/21/14
199	Project 2010-17	Project 2010-17 Definition of Bulk Electric System - Phase 2	BES	Informal	1/29/14	2/27/14	Yes 2/27/14
200	Project 2010-05.1	Project 2010-05.1 Protection System: Phase 1 (Misoperations) - PRC-004-3	PRC-004-3	Formal	1/17/14	3/11/14	Yes 3/2/14

RSC Meeting #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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 #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

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

RSC Meeting #20-2, Agenda Item 4.3: Comment History

(As of 5/7/2020)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted

Note: RSC past comment forms are posted on the NPCC Website under "Standards - Regional Standards Comments."

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

4/10/2020

Type	Document	Description	Comments	Status

NPCC Directory Executive Tracking Summary

Revised: 1/20/2020

	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 considering timeline for 2020 Directory #1 periodic review.	TFCP/TFCO anticipate posting D#1 for conforming A-10 changes Spring 2020.
	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	Special Protection Systems	TFSP	Jul-13	TFSP Reviewing D#7 Criteria; TFCP Coordinating Review of D#7 Appendix B.	Currently Under TFCP and TFSP Review. Anticipate first Open Process posting mid 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		
	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	C-33	Procedure for Analysis and Classification of Dynamic Control Systems	TFSS			Retired by TFSS November 6, 2019.

NPCC Directory Criteria Clarifications

Revised: 1/20/2020 / 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	Pending	TFCO	Pending	Pending	Clarification on Behalf of OPG.	

1/20/2020

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 refeenced 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
Randy MacDonald
Director, Corporate Compliance
Tel. (506) 458-4653
Cell. (506) 470-3536
Email: RaMacDonald@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
Kristina Henderson, CPESC
Lead Analyst – NERC Compliance
89 East Avenue
Rochester, New York 14649
Tel. (585) 771-6153
Email: Kristina.Henderson@avangrid.com

Hydro-Quebec TransÉnergie

Primary
Nicolas Turcotte
Acting Manager – Reliability Standards 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
Caroline Dupuis, ing.
Acting Director – Reliability Standards and Regulatory Compliance
2 Complexe Desjardins, 13th floor, East Tower
Montréal, Québec, Canada H5B 1H7
Tel. (514) 879-4100 Ext: 5903
Email: dupuis.caroline@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

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
Christopher Overberg
Engineer
Tel. (212) 460-2915
Fax (212) 529-1130
Email: overbergc@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. RD20-2-000**

INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION REGARDING STANDARDS DEVELOPMENT PROJECTS

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
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 19, 2020

TABLE OF CONTENTS

I. BACKGROUND 2
II. PROJECT SCHEDULES 3
A. Project 2016-02 Modifications to CIP Standards 3
B. Project 2019-02 BES Cyber System Information Access Management 4
III. CONCLUSION 4

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 the current schedule for both projects.

---

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.

I. BACKGROUND

NERC initiated Project 2016-02 to address the directives from Order No. 822[4] as well as issues identified during implementation of the CIP Reliability Standards approved in Order No. 791.[5] One issue identified during implementation included how the CIP Reliability Standards address virtualization.[6] Because of the increasing use of virtualization in industrial control system environments, the Project 2016-02 standard drafting team is considering modifications to the CIP Reliability Standards and associated definitions to address permitted architecture and the security risks of virtualization technologies.

NERC initiated Project 2019-02 to develop modifications to the CIP Reliability Standards regarding managing access and securing BES Cyber System Information. Specifically, Project 2019-02 seeks to clarify requirements in CIP-004-6 and CIP-011-2 regarding access management of BES Cyber System Information while in transit, storage, and use and to clarify protections when Responsible Entities use third-party cloud service providers for BES Cyber System Information.

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.[7] 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

---

[4] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, at PP 32, 73, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

[5] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

[6] "Virtualization is the process of creating virtual, as opposed to physical, versions of computer hardware to minimize the amount of physical hardware resources required to perform various functions." *Virtualization and Cloud Computing Services*, Notice of Inquiry, 170 FERC ¶ 61,110 at P 4 (2020) (citing the National Institute of Standards and Technology, *Guide to Security for Full Virtualization Technologies, Special Publication* 800-125 (Jan. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf.).

[7] February 20 Order, *supra* note 1, at P 5.

updates, beginning in June 2020, until NERC files new or modified standards with the Commission.[8]

II. PROJECT SCHEDULES

The following section provides the status of the projects, interim target dates, and the anticipated filing dates for modified Reliability Standards for Projects 2016-02 and 2019-02. NERC notes that these schedules are projections and are subject to change. For example, schedules may change based on the comments received in response to the Notice of Inquiry on Virtualization and Cloud Computing Services.[9]

A. Project 2016-02 Modifications to CIP Standards

The Project 2016-02 standard drafting team is proposing virtualization modifications to currently enforceable Reliability Standards CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, and CIP-010-2, with possible conforming changes to other Reliability Standards. The standard drafting team has conducted informal comment periods on these revisions and is currently preparing for a formal comment period and ballot.

The standard drafting team has set the following projected interim target dates:

- Initial 45-day formal comment period and ballot: Posted September 2020
- Additional 45-day formal comment period and ballot (if needed): Posted February 2021
- Additional 45-day formal comment period and ballot (if needed): Posted June 2021
- Final ballot: Posted August 2021
- NERC Board of Trustees Adoption: November 2021

---

8 *Id.*

9 *Virtualization and Cloud Computing Services*, Notice of Inquiry, 170 FERC ¶ 61,110 (2020).

The standard drafting team anticipates filing the proposed Reliability Standards with the Commission in December 2021.

B. Project 2019-02 BES Cyber System Information Access Management

The Project 2019-02 standard drafting team is proposing modifications to currently enforceable Reliability Standards CIP-004-6 and CIP-011-2 to address access management to BES Cyber System Information. The standard drafting team posted the Reliability Standards for an initial 45-day formal comment period and ballot, which did not achieve enough affirmative votes. The standard drafting team is reviewing comments received and is preparing to post for an additional 45-day formal comment period and ballot.

The standard drafting team has set the following projected interim target dates:

- Additional 45-day formal comment period and ballot: Posted May 2020
- Final ballot: Posted August 2020
- NERC Board of Trustees Adoption: August 2020

The standard drafting team anticipates filing the proposed Reliability Standards with the Commission in September 2020.

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 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 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
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 19, 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 19th day of March, 2020.

/s/ Marisa Hecht

Marisa Hecht
Counsel for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. FA11-21-000**

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] submits this compliance filing in accordance with the Commission's January 16, 2013 Order in Docket No. FA11-21-000.[2] In the January 16 Order, the Commission approved a Settlement Agreement between the Office of Enforcement ("Enforcement") and NERC related to Enforcement's findings and recommendations arising out of its 2012 performance audit of NERC. Specifically, Section II.7(b)(i) of the Settlement Agreement requires that:

> Within forty-five days of the end of each quarter, beginning with the quarter ending March 31, 2013, NERC will file with the Commission the unaudited report of the NERC budget-to-actual spending variances during the preceding quarter. This report will include information regarding sources and uses of operating and working capital reserves and will match or exceed the level of detail of the quarterly budget-to-actual variance report of NERC expenditures attached to the agenda of NERC Board of Trustees Finance and Audit Committee's October 2012 meeting.[3]

Attached hereto is the unaudited report of NERC's budget-to-actual variance information for the fourth quarter of 2019, in accordance with the January 16 Order. This variance

---

[1] NERC was certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. FERC certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

[2] *See North American Electric Reliability Corporation, Order Approving Settlement Agreement*, 142 FERC ¶ 61,042 (2013) ("January 16 Order").

[3] *Id.*

information was posted on NERC's website January 30, 2020 and was reviewed at the February 5, 2020 open meeting of the NERC Finance and Audit Committee. The unaudited report was accepted by the NERC Board of Trustees at its meeting on February 6, 2020.

II. NOTICES AND COMMUNICATIONS

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

Meredith M. Jolivert
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
Meredith.jolivert@nerc.net

Andy Sharp
Vice President, Controller
North American Electric Reliability Corporation
3353 Peachtree Road NE, Suite 600 – North Tower
Atlanta, GA 30326
(404) 446-9732
Andy.Sharp@nerc.net

III. DISCUSSION OF SIGNIFICANT VARIANCES BETWEEN 2019 BUDGET AND ACTUAL 2019 RESULTS

The attached fourth quarter 2019 variance report compares actual (unaudited) financial results to NERC's budgeted expenditures as of December 31, 2019. NERC is providing additional discussion of significant variances between the unaudited year-end 2019 results and NERC's 2019 budgeted expenditures by NERC department or program area and by major activity within departments and program areas. This discussion focuses on variances of $500,000 or more between the unaudited year-end 2019 results and the 2019 budget. NERC has focused on year-end variances in excess of budget of $500,000 or more because Section 7(b)(ii) of the Settlement Agreement specifies that NERC will file for Commission review and approval proposals approved by the NERC Board of Trustees to expend $500,000 or more from Operating Reserves designated for "unforeseen contingencies" (as defined in NERC's Working Capital and Operating Reserves Policy), *i.e.*, where any amount allocated from the unforeseen contingencies

account of Operating Reserves plus any amount redirected from previously budgeted funds is, in the aggregate, $500,000 or more for any one specific project or major activity in a program area.

A. Variances of $500,000 or more by Department or Program Area

In late 2018, NERC management went through an organizational assessment, including the alignment of various programs and staffing resources according to roles and responsibilities, and re-characterized several employees across multiple departments. In general, these employees maintained the same responsibilities and functional oversight, but were assigned different managers or departments. In some cases, similar roles were consolidated to align certain technical functions. The changes had no effect on total FTEs (full-time equivalents) for the company, and the net cost impact of these movements was not material to the 2019 budget. However, for financial presentation purposes as it relates to the original 2019 Business Plan & Budget, three of the six affected departments have year-end budget variances over or under $500,000, primarily due to the change in alignment of staffing within and across these program areas: Compliance Assurance; Compliance Analysis, Registration and Certification; and Reliability Assessment and System Analysis. As of December 31, 2019, Compliance Assurance is over budget by $929,876, Compliance Analysis, Registration and Certification is under budget by $998,476, and Reliability Assessment and System Analysis is under budget by $944,923. Other departments and program areas reflect over and under budget amounts as well resulting from this reorganization, but none were greater than $500,000.

Compliance Enforcement was under budget by $547,823 primarily due to lower personnel and contracts and consultants expenses. Legal and Regulatory is over budget by $1,104,921 primarily due to transition costs and search fees as well as Internal Audit expenditures that were budgeted in the Finance and Accounting department and were charged to

the Legal and Regulatory department. CRISP is projected to be under budget by $1,087,041 primarily due to lower personnel, software and contractor costs, which will be partially offset by lower third-party funding required from CRISP participants.

IV. CONCLUSION

NERC respectfully requests that the Commission accept this filing as compliant with Section II.7(b)(i) of the Settlement Agreement and the Commission's January 16 Order in Docket No. FA11-21-000.

Respectfully submitted,

/s/ Meredith M. Jolivert

Meredith M. Jolivert
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
meredith.jolivert@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: February 14, 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 14th day of February, 2020.

/s/ Meredith M. Jolivert

Meredith M. Jolivert
Counsel for North American Electric Reliability Corporation

ATTACHMENT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Summary of Unaudited Results For the Month Ending December 31, 2019

Table of Contents

		Page
1.	Executive Summary	
	a. Year-to-Date Actual Results	2
2.	Detailed Operating Results	
	a. Variances by Revenue and Expense Category	3
	b. Variances by Department	5
3.	Supplemental Schedules	
	a. Schedule 1 – Year-End Actual Reserves	7
	b. Schedule 2 – IT Projects	8
	c. Schedule 3 – E-ISAC & CRISP Summary of Activity	11

Executive Summary

Year-to-Date Actual Results
($ millions)

FUNDING	Actual	Budget	Over (Under)
Revenues	$ 78.8	$ 78.5	$ 0.3
Funding from Reserves			
Assessment Stabilization Reserve	0.6	0.6	-
TOTAL FUNDING	**$ 79.4**	**$ 79.1**	**$ 0.3**
EXPENDITURES			
Expenses (excluding Depreciation)	$ 75.1	$ 75.2	$ (0.1)
Fixed Asset Additions	3.6	4.8	(1.2)
TOTAL EXPENDITURES	**$ 78.7**	**$ 80.0**	**$ (1.3)**
RESERVE INCREASE (DECREASE)	**$ 0.7**	**$ (0.9)**	**$ 1.6**

Funding

- Revenues
  - Slightly over budget mainly due to higher than budgeted workshop revenues and investment income, which is offset by lower third party revenues required to fund the CRISP program.

Expenditures

- Expenses (excluding depreciation)
  - Personnel expenses are over budget largely because of transition costs and search fees.
  - Meeting expenses are over budget primarily due to higher participation in workshops, which were substantially offset by higher than budgeted workshop revenues.
  - Contracts and Consultants expenses are under budget primarily due to lower than expected spending in the Reliability Assessment and System Analysis and CRISP departments.
  - Professional services expenses are lower than budget largely due to lower legal fees.
- Fixed Asset Additions
  - Under budget mainly because of lower spending to offset increased costs in other areas, as well some costs that were budgeted in fixed assets but for which the costs were charged to software licenses and support due to the type of license acquired.

Operating Reserve Increase (Decrease)

- Actual reserve increase from operations was higher than budget by $1.6 million.

Detailed Operating Results

Variances by Revenue and Expense Category

Total NERC (including CRISP)

	YTD Actual	YTD Budget	YTD Over (Under)	% Over (Under)
TOTAL FUNDING	**$ 79,345,605**	**$ 79,130,349**	**$ 215,257**	**0.3%**
EXPENDITURES				
Personnel	$ 44,610,615	$ 43,952,190	$ 658,425	1.5%
Meetings, Travel, and Conference Calls	4,203,281	3,380,400	822,881	24.3%
Contracts and Consultants	13,694,112	15,043,318	(1,349,206)	(9.0%)
Rent and Facilities	3,312,254	3,335,058	(22,804)	(0.7%)
Office Costs, Professional, and Misc.*	9,241,842	9,346,517	(104,675)	(1.1%)
Other Non-Operating Expenses	2,717	214,171	(211,454)	(98.7%)
Fixed Asset Additions*	3,623,136	4,778,000	(1,154,864)	(24.2%)
TOTAL EXPENDITURES	**$ 78,687,957**	**$ 80,049,655**	**$ (1,361,698)**	**(1.7%)**
RESERVE INCREASE (DECREASE)	**$ 657,649**	**$ (919,306)**	**$ 1,576,954**	**(171.5%)**
FTEs	**201.8**	**204.9**	**(3.1)**	**(1.5%)**

***** Excludes depreciation expense

Following is a brief summary of variances by category:

- Personnel Expense
  - Over budget primarily due to transition costs and search fees.
- Meeting, Travel, and Conference Call Expense
  - Meeting expenses are over budget primarily due to higher participation in workshops, which were substantially offset by higher than budgeted workshop revenues.
- Contracts and Consultants Expense
  - Under budget due to lower than expected spending primarily in the Reliability Assessment and System Analysis and CRISP departments. Also, amounts for Internal Audit projects that were originally budgeted in the Finance and Accounting department were charged to the Legal and Regulatory department, which nets to a $26k over budget amount between those departments.

CONTRACTS and CONSULTANTS	YTD Actual	YTD Budget	YTD Over (Under)
Reliability Standards	$ -	$ 50,000	$ (50,000)
Compliance Assurance	-	50,000	(50,000)
Compliance Analysis, Registration and Certification	-	-	-
Compliance Enforcement	56,263	161,000	(104,738)
Reliability Assessment and System Analysis	265,435	625,000	(359,565)
Situation Awareness	1,387,476	1,280,990	106,486
Event Analysis	-	-	-
Performance Analysis	677,854	653,565	24,289
E-ISAC	1,811,592	1,820,500	(8,908)
Training, Education, and Personnel Certification	498,683	497,000	1,683
General and Administrative and Executive	162,524	220,000	(57,477)
Legal and Regulatory	356,412	-	356,412
Policy and External Affairs	19,037	20,000	(963)
Information Technology	1,861,913	2,042,763	(180,850)
Human Resources and Administration	677,551	690,000	(12,449)
Finance and Accounting	93,498	475,000	(381,502)
TOTAL (excluding CRISP)	**$ 7,868,238**	**$ 8,585,818**	**$ (717,580)**
CRISP	5,825,874	6,457,500	(631,626)
TOTAL (including CRISP)	**$ 13,694,112**	**$ 15,043,318**	**$ (1,349,206)**

- Other Non-Operating Expenses
  - Under budget due to the anticipated refund of prior and current year excise taxes due to recent tax law changes.
- Fixed Asset Additions
  - Under budget mainly because of lower spending to offset increased costs in other areas, as well some costs that were budgeted in fixed assets but for which the costs were charged to software licenses and support due to the type of license acquired.

Variances by Department

DIRECT EXPENSES and NET FIXED ASSETS	YTD Actual	YTD Budget	YTD Over (Under)
Reliability Standards	$ 3,547,529	$ 3,419,581	$ 127,948
Compliance Assurance	6,108,382	5,178,505	929,876
Compliance Analysis, Registration and Certification	1,883,328	2,881,804	(998,476)
Compliance Enforcement	3,313,867	3,861,690	(547,823)
Reliability Assessment and System Analysis	3,661,184	4,606,107	(944,923)
Situation Awareness	3,104,458	3,012,404	92,054
Event Analysis	2,754,180	2,771,658	(17,478)
Performance Analysis	3,315,040	2,873,967	441,072
E-ISAC	10,517,482	10,649,090	(131,608)
Training, Education, and Personnel Certification	1,479,464	1,367,755	111,709
General and Administrative and Executive	8,262,192	8,144,200	117,992
Legal and Regulatory	4,983,712	3,878,791	1,104,921
Policy and External Affairs	2,412,714	2,510,721	(98,007)
Information Technology	11,214,035	11,696,532	(482,497)
Human Resources	2,590,220	2,562,371	27,848
Finance and Accounting	2,546,483	2,553,747	(7,265)
TOTAL (excluding CRISP)	**$ 71,694,269**	**$ 71,968,925**	**$ (274,656)**
CRISP	6,993,688	8,080,729	(1,087,041)
TOTAL EXPENSES and NET FIXED ASSETS	**$ 78,687,957**	**$ 80,049,655**	**$ (1,361,698)**

In late 2018, NERC management went through an organizational assessment involving various program areas and re-characterized several employees across multiple departments. In most cases, these employees kept the same responsibilities and functional oversight, but were assigned new departments and/or consolidated with other similar roles to align certain technical functions. The changes had no effect on the total FTEs, and the net cost impact of these movements was immaterial. The following program areas were impacted by this review:

- Reliability Standards
- Compliance Assurance
- Compliance Analysis, Registration and Certification
- Reliability Assessment and System Analysis
- Event Analysis
- Performance Analysis

Following is a brief summary of variances by department:

- Legal and Regulatory – Over budget at year-end primarily due to transition costs and search fees, as well as Internal Audit expenditures that were budgeted in the Finance and Accounting department that were charged to the Legal and Regulatory department.
- Information Technology – Under budget, mainly due to lower fixed asset spending, which was partially offset by higher personnel costs due to a lower attrition rate, as well as CMEP and other costs that were funded by IT and charged to program areas.
- CRISP – Under budget largely because of lower personnel, software, and contractor costs.

Supplemental Schedules

Schedule 1 – Year-End Actual Reserves

Reserve Account	Beginning Balance [1]	Budgeted Funding	Budgeted Uses	Other Funding (Uses) [2]	Net Financing Activity [3]	Ending Balance
Operating Contingency	**$ 5,644,359**	$ 550,000	$ (1,067,980)	$ 1,027,127	$ (394,688)	**$ 5,758,818**
Future Obligations	**2,535,333**	-	(480,457)	64,843	-	**2,119,719**
Assessment Stabilization	**2,071,000**	-	(550,000)	1,000,000	-	**2,521,000**
System Operator	**592,110**	148,674	-	(172)	-	**740,611**
CRISP	**500,000**	-	-	-	-	**500,000**
Total Reserves	**$ 11,342,801**	$ 698,674	$ (2,098,437)	$ 2,091,798	$ (394,688)	**$ 11,640,148**

NOTES:

(1) Some 2019 beginning balances have been adjusted from the 12/31/2018 variance report balances as the result of a reconciliation to the final audited balance sheet.

(2) The column Other Funding (Uses) primarily reflects the net impact of normal operations. For example, under normal circumstances, if NERC was tracking well under budget in actual expenditures, this would reflect additional funds into the reserve account. It also reflects the increase or decrease in working capital during the period.

(3) Net financing activity in 2019 reflects principal debt repayments for borrowings originating in 2016. NERC did not make budgeted borrowings for 2017, 2018, and 2019 in light of a favorable working capital position. The savings from the 2019 borrowing decision will be realized in the years 2020 to 2022.

Schedule 2 – IT Projects

Projects in Progress	Project Budget [1]	Actual Spend	Expected Spend	Expected Over (Under) Budget
CMEP Technology Project (2017-2020)	$ 5,403,000	$ 3,485,314	$ 5,484,524	$ 81,524
Standards (2019-2020)	300,000	266,723	300,000	-
Windows 10 Upgrade	169,890	129,890	169,890	-

Projects Completed in 2019	Project Budget [1]	Actual Spend	Actual Over (Under) Budget
FRCC Dissolution	$ 128,497	$ 122,238	$ (6,259)
Multifactor Authentication	27,660	7,173	(20,488)
Footprints Upgrade	84,753	60,600	(24,153)
E-ISAC - Customer Relationship Management (CRM)	237,800	285,229	47,429
Entity Registration - CORES (2018-2019)	1,200,000	1,252,919	52,919
Document Management - Records Center Reconfiguration	190,500	190,500	-
SAFNR V3	221,500	188,000	(33,500)

NOTES:

(1) The Project Budget noted above usually corresponds to the approved business case for each project and funds for each project are drawn from the available budget. In some projects, business cases may not be prepared, particularly when a project is smaller and/or may be in response to a FERC order.

** Some of these projects span multiple years, so the amounts above do not represent a single budget year expenditure.*

** The amounts noted above do not include internal labor or license/maintenance/support costs and reflect only external (consultant) costs of the projects.*

Schedule 2 (continued) – IT Projects

CMEP Technology Project
(Started May 2017 / Planned Completion Q4 2021)
This project will provide registered entities, Regional Entities, and NERC the ability manage the compliance and enforcement processes and data in a single ERO Enterprise system. Today, those processes and related data are managed across three separate systems that have to be synchronized (webCDMS, CITS, and CRATS).

Standards
(Started Jan 2019 / Planned Completion Q4 2020)
In support of the CMEP Technology Project, this project involves the movement all of the Standards data from the old source system to the new one.

Microsoft Windows 10
(Started Dec 2019 / Planned Completion Feb 2020)
This project involves the upgrade of all laptops and desktops from Windows 7 to Windows 10. This upgrade will provide a more secure environment. Microsoft stopped support of Windows 7 security patches in January 2020.

FRCC Dissolution
(Started Jan 2019 / Completed Jul 2019)
With FRCC dissolving, NERC assessed the changes required to applications that contained FRCC data and the reassignment/classification of such information. The inventory required the mapping utility, functionality, migration, and support efforts by both Region and entity. Activities included facilitated discussions with IT and business owners of impacted applications to capture and document high-level, as well as more detailed, requirements necessary to support the transition of registered entities from FRCC to SERC.

Multifactor Authentication
(Started Jan 2019 / Completed Jul 2019)
The purpose of this project was to implement a Multi-Factor Authentication solution to enhance the overall security of the NERC ERO suite of applications and to meet existing requirements for applications currently under development, primarily CORES and CMEP/Align projects. Multi-factor authorization provides enhanced security by requiring more than one method of user authentication (Mobile PIN code, etc.) in addition to the traditional user name/password authentication method.

Schedule 2 (continued) – IT Projects

Footprints Upgrade
(Started Mar 2019 / Completed Aug 2019)
The purpose of this project was to replace the current version of the NERC IT helpdesk ticketing system, Footprints v11, with the latest version available, Footprints v12. The Footprints application manages NERC internal IT support requests. The implemented version enables support of ERO applications (i.e. CORES, ALIGN, etc.) by distributed regional support teams.

E-ISAC – Customer Relationship Management (CRM)
(Started Jul 2019 / Completed Oct 2019)
The purpose of this project was to select and implement a Customer Relationship Management (CRM) tool to assist the E-ISAC team in growing its North American electricity owner/operator base from the current roughly 1,000 members to a progressively greater share of the roughly 5,000 total. The team will be able to do so through improved outreach, marketing, and overall engagement and tracking processes expected from use of the new tool. The plan is also to integrate with the E-ISAC Portal in the future.

Entity Registration - CORES
(Started Dec 2017 / Completed Nov 2019)
NERC undertook an effort to both standardize and modernize the Entity Registration process. The discovery phase of the Centralized Organization Registration Entity System (CORES) project included the capture of Region-specific needs, variations, and exceptions in the registration process. CORES is a centralized entity registration process, which requires the retirement of registration in CDMS, CITS, and CRATS. The Joint Registration Organization (JRO) portion of the project was combined with the CORES production release in 2019.

Document Management – Records Center Reconfiguration
(Started May 2019 / Completed Dec 2019)
The Records Retention project is in alignment with the original intent and business case for Document Management. One of the key items for addressing information management across all program areas was to have the ability to address retention and destruction of documents identified as NERC records. The objective of the project was to implement a solution to identify NERC records and their respective disposition rules in in accordance with the NERC Records Retention and Destruction policy.

SAFNR V3
(Started May 2019 / Completed Dec 2019)
One of the primary functions of the ERO Enterprise is to maintain situational awareness of Bulk Power System conditions and provide accurate and timely information regarding threats that may adversely impact reliability. The objective of this project was to identify a new vendor and platform to replace the existing Situation Awareness for FERC, NERC, and the Regional Entities system, SAFNR V2. The new platform not only supports NERCS goal to reduce reliability risk by providing situation awareness of the Bulk Power System but also provides new features and architectural/infrastructure enhancements to increase productivity and availability.

Schedule 3 – E-ISAC and CRISP Summary of Activity

TOTAL E-ISAC (including CRISP)

FUNDING	Annual Actual	Annual Budget	Over (Under)
Assessments	$ 19,627,897	$ 19,627,897	$ 0
Other Funding	7,641,896	7,767,730	(125,834)
TOTAL FUNDING	$ 27,269,793	$ 27,395,627	$ (125,834)
EXPENDITURES			
Personnel Expense	$ 7,551,161	$ 8,180,123	$ (628,962)
Meeting Expense	957,187	418,000	539,187
Operating Expenses (excluding Depreciation)	8,698,738	9,431,696	(732,958)
Other Non-Operating Expenses	10,467	-	10,467
Fixed Assets (excluding Depreciation and Fixed Asset Allocation)	293,615	700,000	(406,384)
Total Direct Costs (excluding Depreciation and Allocations)	$ 17,511,169	$ 18,729,819	$ (1,218,650)
Indirect Expense Allocation	8,674,257	9,004,572	(330,314)
Fixed Asset Allocation	(368,481)	(338,764)	(29,717)
TOTAL EXPENDITURES (excluding Depreciation, including Allocations)	$ 25,816,946	$ 27,395,627	$ (1,578,681)
RESERVE INCREASE (DECREASE)	$ 1,452,847	$ -	$ 1,452,847

Schedule 3 (continued) – E-ISAC and CRISP Summary of Activity

CRISP

FUNDING	Annual Actual	Annual Budget	Over (Under)
Assessments	$ 1,526,388	$ 1,526,388	$ 0
Other Funding	6,994,273	7,517,319	(523,046)
TOTAL FUNDING	$ 8,520,661	$ 9,043,707	$ (523,046)
EXPENDITURES			
Personnel Expense	$ 729,670	$ 965,793	$ (236,123)
Meeting Expense	90,500	48,000	42,500
Operating Expenses (excluding Depreciation)	6,036,086	6,966,936	(930,850)
Other Non-Operating Expenses	10,467	-	10,467
Fixed Assets (excluding Depreciation and Fixed Asset Allocation)	126,964	100,000	26,964
Total Direct Costs (excluding Depreciation and Allocations)	$ 6,993,688	$ 8,080,729	$ (1,087,041)
Indirect Expense Allocation	981,943	1,000,605	(18,662)
Fixed Asset Allocation	(41,713)	(37,628)	(4,085)
TOTAL EXPENDITURES (excluding Depreciation, including Allocations)	$ 7,933,918	$ 9,043,707	$ (1,109,789)
RESERVE INCREASE (DECREASE)	$ 586,743	$ -	$ 586,743

E-ISAC (excluding CRISP)

FUNDING	Annual Actual	Annual Budget	Over (Under)
Assessments	$ 18,101,509	$ 18,101,509	$ 0
Other Funding	647,623	250,411	397,212
TOTAL FUNDING	$ 18,749,132	$ 18,351,920	$ 397,212
EXPENDITURES			
Personnel Expense	$ 6,821,491	$ 7,214,330	$ (392,839)
Meeting Expense	866,687	370,000	496,687
Operating Expenses (excluding Depreciation)	2,662,652	2,464,760	197,892
Other Non-Operating Expenses	-	-	-
Fixed Assets (excluding Depreciation and Fixed Asset Allocation)	166,652	600,000	(433,348)
Total Direct Costs (excluding Depreciation and Allocations)	$ 10,517,482	$ 10,649,090	$ (131,608)
Indirect Expense Allocation	7,692,314	8,003,966	(311,652)
Fixed Asset Allocation	(326,768)	(301,136)	(25,632)
TOTAL EXPENDITURES (excluding Depreciation, including Allocations)	$ 17,883,028	$ 18,351,920	$ (468,892)
RESERVE INCREASE (DECREASE)	$ 866,104	$ -	$ 866,104

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RR19-7-000**

MOTION FOR EXTENSION OF COMPLIANCE FILING DEADLINE OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO THE ORDER ON THE FIVE-YEAR PERFORMANCE ASSESSMENT

On January 23, 2020, the Federal Energy Regulatory Commission ("Commission") issued an order on the North American Electric Reliability Corporation's ("NERC") Five-Year Performance Assessment ("Order").[1] In this Order, the Commission accepted NERC's Performance Assessment and directed NERC to submit two compliance filings. The first compliance filing is due April 22, 2020 and the second compliance filing is due July 21, 2020 ("July Compliance Filing"). The July Compliance Filing requires NERC to submit revisions to its Rules of Procedure ("ROP") to correct inconsistent E-ISAC terminology,[2] to provide more transparency in its sanction guidelines,[3] and to address various elements of the certification program.[4]

Pursuant to Rules 212 and 2008 of the Commission's Rules of Practice and Procedure,[5] NERC submits this motion requesting extension of the July Compliance Filing deadline. Specifically, NERC requests that the Commission extend the deadline of the July Compliance Filing from July 21, 2020 to August 28, 2020. Extending the compliance filing deadline to August

[1] *See Order on Five-Year Performance Assessment*, 170 FERC ¶ 61,029 (2020) ("Order").

[2] *Id*. at PP 73-74.

[3] *Id*. at PP 77-80.

[4] *Id*. at PP 84-87.

[5] 18 C.F.R. §§ 385.212 & 385.2008 (2019); *NERC Rules of Procedure*, https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx (effective January 29, 2019).

28, 2020 would provide NERC with sufficient time to follow its procedure to post proposed ROP revisions for public comment, as required in the NERC Bylaws.[6] An extension of the deadline would also allow NERC to include the Commission-directed ROP changes related to the certification program to an ongoing ROP project examining enhancements to the registration and certification program.

I. Motion for Extension of Time

NERC respectfully requests an extension of the July Compliance Filing deadline from July 21, 2020 to August 28, 2020, to comply with the Commission's directive to enhance provisions of the ROP relating to the E-ISAC, the sanction guidelines, and the certification program. Good cause exists to grant this extension. In particular, the requested extension of time will allow NERC to follow its internal notice and comment procedures prior to submitting the proposed ROP revisions to the NERC Board of Trustees ("Board"). The extension of time will also allow NERC to present a complete set of registration and certification ROP revisions, which were in development prior to the Commission's issuance of the Order.

Extending the deadline for the July Compliance Filing will allow NERC sufficient time to ensure transparency in developing revisions to the ROP. After NERC completes the drafting of its revisions, NERC will provide notice to stakeholders by posting the revisions on the NERC website. Once proposed revisions are posted, stakeholders are given a 45-day comment period to provide feedback on the ROP revisions. After the 45-day comment period, NERC may post the revisions for additional comment based on the nature and quantity of the revisions. NERC must justify its response to stakeholder comments, including when NERC chooses not to accept a revision

[6] *See NERC Bylaws,* https://www.nerc.com/gov/Annual%20Reports/NERC%20Bylaws_Effective%20September%2025,%202018.pdf (effective September 25, 2018).

suggested by a stakeholder. NERC's responses to comments are posted on the NERC website. NERC must then provide the Board with sufficient time, generally 15 days, to review the proposed ROP revisions (including the consideration of comments) before the Board meeting. The current compliance deadline would require NERC to complete its ROP revisions and its notice and comment procedure for the May 13, 2020 Board meeting. NERC believes that it is more feasible to complete its process and submit the proposed revisions for the August 20, 2020 Board meeting.

Also, prior to the Commission's issuance of the Order, NERC was working on a broader scope of ROP changes to its registration and certification program. Particularly, NERC was working with the Regional Entities, stakeholders, and the Compliance and Certification Committee ("CCC") to enhance the registration and certification sections of the ROP. These ROP enhancements were initiated in response to the implementation of risk-based registration five years ago. This ongoing ROP project addresses a much wider scope of registration and certification changes than the Commission's directive. NERC will continue to develop ROP revisions to address the Commission-directed certification program in coordination with the Regional Entities, stakeholders and the CCC.

II. Conclusion

For the forgoing reasons, NERC respectfully requests that the Commission grant this motion and extend the deadline for NERC's July Compliance Filing to August 28, 2020.

Respectfully submitted,

/s/ Alain Rigaud

Nina Jenkins-Johnson
Senior Counsel
Alain Rigaud
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
Nina.johnston@nerc.net
Alain.rigaud@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 21, 2020

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 4, 2020

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

ATTN: Andrew Dodge, Director, Office of Electric Reliability

Re: Request for Additional Time to Respond to Data Request
North American Electric Reliability Corporation, Western Electricity Coordinating Council
Docket No. RM19-20-000

Dear Mr. Dodge:

The North American Electric Reliability Corporation ("NERC") and Western Electricity Coordinating Council ("WECC") hereby request an additional 45 days to respond to the data request issued in the above-referenced docket on February 18, 2020.[1]

On September 6, 2019, NERC and WECC filed a joint petition with the Commission for approval of proposed regional Reliability Standard BAL-002-WECC-3 (Contingency Reserve), in which Requirement R2 of the currently effective standard is proposed to be retired.[2] In this petition, NERC and WECC stated that Requirement R2 is now redundant to the continent-wide frequency response standard and, based on the results of a one-year field test performed by WECC from May 1, 2017 to April 30, 2018, WECC determined that retirement of Requirement R2 would have no adverse impact on reliability in the Western Interconnection.

On February 18, 2020, the Commission, pursuant to authority delegated to the Director of the Office of Electric Reliability, issued a data request seeking additional information within 30 days. Specifically, the data request seeks:

[1] *Data Request in Response to Joint Petition Seeking Approval of Regional Reliability Standard BAL-002-WECC-3*, Docket No. RM19-20-000 (Feb. 18, 2020).

[2] *Petition of NERC and WECC for Approval of Proposed Regional Reliability Standard BAL-002-WECC-3*, Docket No. RM19-20-000 (Sep. 6, 2019).

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

- The following data, from April 30, 2018 through September 30, 2019: (1) for any reportable Disturbance Control Standard ("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; and (2) for events involving a loss of 700 megawatts ("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 loss.

- The amount of spinning reserve above or below 50 percent during non-event times on an hourly basis from May 1, 2017 through September 30, 2019.

- Supporting data for NERC frequency response metric (M-4) as it pertains to the Western Interconnection from May 1, 2017 through September 30, 2019.

NERC and WECC respectfully request that the Commission grant NERC and WECC an additional 45 days to submit the requested information. WECC and NERC believe they have the ability to obtain all or most of the requested data; however, the process of collecting the data will take additional time beyond the 30 days originally provided for response.

As NERC and WECC noted in their September 6 joint petition, WECC, with NERC approval, provided a compliance waiver for Requirement R2 to responsible entities in order to conduct the one-year field test.[3] After it was determined that Requirement R2 should be retired, the compliance waiver was extended to allow for the completion of the regulatory approval process.

Following the conclusion of the field test, WECC did not continue to collect the information that it collected during the field test. WECC, therefore, must obtain this data from the entities that possess it. In some cases, as the responsible entities had been granted a compliance waiver, the Reserve Sharing Group will need to request the amount of Operating Reserve – Spinning being carried from some Balancing Authorities, which could take additional time. An unrelated transition in Reserve Sharing Groups in the Interconnection after the conclusion of the field test could also cause a delay in certain data being provided to WECC.

Under the circumstances, NERC and WECC submit that a 45-day extension of time is appropriate and reasonable and respectfully request that the Commission grant the request. If granted, NERC and WECC would file a response to the data request by no later than Monday, May 4, 2020.

[3] *Id*. at 13.

Respectfully submitted,

/s/ Lauren A. Perotti
Senior Counsel
North American Electric Reliability Corporation
1325 G St., NW, Suite 600
Washington, DC 20005
202-400-3000
lauren.perotti@nerc.net

Counsel for the North American Electric Reliability Corporation

Steve Goodwill
Senior Vice President, General Counsel, and Corporate Secretary
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
sgoodwill@wecc.org

Counsel for the Western Electricity Coordinating Council

Cc: Syed Ahmad, Office of Electric Reliability
Syed.Ahmad@ferc.gov

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 4th day of March, 2020.

/s/ Lauren A. Perotti

Lauren A. Perotti

Counsel for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Michael Mabee	**)**	**Docket No. EL20-21-000**
Complainant	**)**	
	)	
v.	**)**	
	)	
Federal Energy Regulatory Commission	**)**	

MOTION TO INTERVENE AND COMMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

James McGrane
Senior Counsel
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Lauren 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
james.mcgrane@nerc.net
ed.kichline@nerc.net
lauren.perotti@nerc.net

Counsel for the North American Electric Reliability Corporation

March 2, 2020

TABLE OF CONTENTS

I. NOTICES AND COMMUNICATIONS 2
II. MOTION TO INTERVENE 2
III. SUMMARY 4
A. Summary of the Complaint 4
B. Summary of NERC's Comments 5
IV. COMMENTS 6
A. The Complainant Has Failed to Demonstrate That Reliability Standard CIP-014-2 is Inadequate or is Otherwise Inconsistent With Applicable Statutory and Regulatory Law. 6
B. The Complainant Has Failed to Demonstrate That Enforcement of Reliability Standard CIP-014-2 is Inadequate. 11
C. The Commission is Already Evaluating the Adequacy of Registered Entities' Compliance with Reliability Standard CIP-014-2. 17
V. CONCLUSION 18

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Michael Mabee	**)**	**Docket No. EL20-21-000**
Complainant	**)**	
	)	
v.	**)**	
	)	
Federal Energy Regulatory Commission	**)**	

MOTION TO INTERVENE AND COMMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pursuant to Rules 206, 212, and 214 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Rules of Practice and Procedure[1] and the Commission's Notice of Complaint,[2] the North American Electric Reliability Corporation ("NERC") moves to intervene and comment on the Complaint filed by Michael Mabee ("Complainant") on January 30, 2020 in the above-captioned docket ("Complaint") and the Additional Information and Recommendations of Complainant ("Supplemental Complaint") filed by Complainant on February 19, 2020.

The Complaint and Supplemental Complaint claim that (i) the NERC Reliability Standard CIP-014-2, which addresses physical security of applicable Transmission stations and substations as well as their associated primary control centers, is inadequate; and (ii) that enforcement of the CIP-014-2 Reliability Standard seems nonexistent, and recommend that the Commission take several specified actions, including directing NERC to take specific actions, to address the Complainant's concerns.

[1] 18 C.F.R. §§ 385.206, 385.212, and 285.214 (2019).
[2] Notice of Complaint, Docket No. EL20-21-000 (Feb. 6, 2020).

As discussed below, NERC requests leave to intervene and comment in response to the Complainant's assertions and recommendations, and requests that the Commission dismiss the Complaint.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[3]

James McGrane*
Senior Counsel
Edwin G. Kichline*
Senior Counsel and Director of Enforcement Oversight
Lauren 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
james.mcgrane@nerc.net
ed.kichline@nerc.net
lauren.perotti@nerc.net

II. MOTION TO INTERVENE

NERC has a substantial interest in this proceeding as the Complainant seeks to have the Commission direct NERC to modify the CIP-014-2 Reliability Standard and submit to the Commission for approval a compliance and enforcement plan for physical security.[4] By enacting

[3] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203, to allow the inclusion of more than two persons on the service list in this proceeding.

[4] Complaint at 7. The Complainant's last request for relief does not affect NERC directly, but as discussed in more detail in Section IV.C below, publicly available documents make clear that the Commission is already reviewing registered entities' compliance with CIP-014-2 independently, or in coordination with NERC, in a manner similar to that requested by Complainant.

the Energy Policy Act of 2005,[5] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System ("BPS"), and with the duties of certifying an Electric Reliability Organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. The Commission certified NERC as the ERO for the purpose of establishing and enforcing Reliability Standards for the BPS in the United States.[6] As the ERO, NERC's mission is to improve the reliability and security of the BPS in North America.[7] Under its FERC-approved Rules of Procedure, NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of the NERC Rules of Procedure ("ROP") and the NERC Standard Processes Manual ("SPM").[8] NERC and the Regional Entities are responsible for monitoring, assessing, and enforcing 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 ("CMEP").[9]

No other party can adequately represent NERC's interests or adequately respond to Complainant's allegations regarding the adequacy of the CIP-014-2 Reliability Standard and its enforcement. Therefore, it is in the public interest to permit this intervention.

---

5 16 U.S.C. § 824o (2018).

6 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, *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) ("ERO Certification Order").

7 *See id.*

8 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.

9 *Id*. The NERC Compliance Monitoring and Enforcement Program is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_06082018.pdf.

III. SUMMARY

A. Summary of the Complaint

The Complainant alleges that the CIP-014-2 Reliability Standard is inadequate and that enforcement of the CIP-014-2 Reliability Standard seems nonexistent.[10] The Complainant recommends that the Commission:

i. direct NERC to modify CIP-014-2 such that the entity's physical security plan be effective and receive regulatory approval, and that all risk assessments, evaluations, and security plans should be reviewed by qualified non-affiliated persons with expertise in physical security;

ii. direct NERC to submit to the Commission for approval a compliance and enforcement plan for physical security that would provide "meaningful assurances that the regulators and regulated entities are taking seriously their obligations to protect the bulk power system from physical threats;" and

iii. collaborate with the Department of Energy, Department of Homeland Security, Department of Defense, and the National Guard to "Red Team"[11] entities in order to evaluate weaknesses and determine whether their physical (and cybersecurity) programs are effective, and work with state public utility commissions ("PUCs") to ensure similar actions at the state level.[12]

---

[10] NERC notes that the Complainant, as a private citizen, is not subject to the NERC Reliability Standards, including CIP-014-2.

[11] In this context, to "Red Team" an entity means to perform an adversarial perspective of the entity's physical security plans, risk assessments, and evaluations.

[12] Complaint at 7.

B. Summary of NERC's Comments

In response to the Complaint and Supplemental Complaint, NERC provides the following:

i. The Complainant has failed to demonstrate that Reliability Standard CIP-014-2 is inadequate or is otherwise inconsistent with applicable statutory and regulatory law;

ii. The Complainant has failed to demonstrate that enforcement of Reliability Standard CIP-014-2 is inadequate; and

iii. The Commission is already evaluating the adequacy of registered entities' compliance with Reliability Standard CIP-014-2.

Therefore, the Commission should dismiss the Complaint and Supplemental Complaint because they fail to meet the minimum requirements applicable to complaints under the Commission's Rules of Practice and Procedure,[13] and reflect unsupported assertions that embody the Complainant's misunderstanding of the NERC Standards Development Process and the NERC Compliance Monitoring and Enforcement Program. Rule 203, for example, requires pleadings to set forth the basis in fact and law for the positions taken.[14] Rule 206 provides that complaints must, among their elements, (i) clearly identify the alleged action or inaction claimed to violate applicable statutory or regulatory requirements, (ii) set forth the business, commercial, economic, or other issues presented by the action or inaction "as such relate to or affect the complainant," and (iii) make a good faith effort to quantify the financial impact or burden created for the

[13] *See* 18 C.F.R. § 385.206.

[14] 18 C.F.R. § 385.203(a)(7).

complainant due to the action or inaction.[15] Long-standing Commission precedent provides that "rather than bald allegations, [a complainant] must make an adequate proffer of evidence including pertinent information and analysis to support its claims."[16]

IV. COMMENTS

A. The Complainant Has Failed to Demonstrate That Reliability Standard CIP-014-2 is Inadequate or is Otherwise Inconsistent With Applicable Statutory and Regulatory Law.

The Complaint asserts that Reliability Standard CIP-014-2 is inadequate and requests that the Commission direct further modifications to the standard. The Complainant has failed to meet its burden under the Commission's rules. NERC developed Reliability Standard CIP-014-2, and its predecessor standard CIP-014-1, in accordance with its open and inclusive, Commission-approved standard development process.[17] Following its own public processes, the Commission found that the standards addressed its directives and approved Reliability Standards CIP-014-1 and CIP-014-2 as just, reasonable, not unduly discriminatory, and in the public interest. The Complaint fails to provide a factual basis to substantiate the claim that the CIP-014 Reliability Standard is now inadequate, nor does it identify any deficiencies in the applicable statutory and

---

[15] 18 C.F.R. § 385.206(b)(1), (3), and (4) (listing the full list of elements for a complaint). NERC does not waive objection to the Complaint's failure to meet other elements of a properly pleaded complaint, but is simply highlighting these elements.

[16] *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 P2 (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).

[17] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual, available at available at https://www nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

regulatory processes used for its development and approval. For these reasons, the Commission should dismiss the Complaint.

The CIP-014 Reliability Standard was developed to respond to Commission directives and was approved in accordance with applicable regulations. On March 7, 2014, the Commission issued an order directing NERC to develop a physical security Reliability Standard.[18] Reliability Standard CIP-014-1 was developed in response to the Commission's directive, using an abbreviated standard development process permitted under NERC's Rules of Procedure.[19] As explained in detail in NERC's petition for approval of the standard,[20] Reliability Standard CIP-014-1 addressed each of the Commission's directives in the March 7 Order. Specifically, Reliability Standard CIP-014-1, and its successor version CIP-014-2, requires owners and operators of the Bulk-Power System to:

- "***perform a risk assessment of their systems to identify their 'critical facilities;'***"[21] specifically, by performing a risk assessment of their systems to identify (i) their critical Transmission stations and Transmission substations, and (ii) the primary control centers that operationally (i.e., physically) control the identified Transmission stations and Transmission substations (Requirement R1);
- "***evaluate the potential threats and vulnerabilities to those identified facilities;***"[22] specifically, by evaluating the potential threats and vulnerabilities of a physical attack to the facilities identified in the risk assessment (Requirement R4); and
- "***develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security***;"[23] specifically, by developing and implementing a security plan, based on the evaluation of threats and vulnerabilities, designed to protect

---

[18] *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, 146 FERC ¶ 61,166 (2014) [hereinafter March 7 Order].

[19] For a description of the abbreviated process, see the NERC Standard Processes Manual, Section 16.0 (Waiver).

[20] *Petition of NERC for Approval of Reliability Standard CIP-014-1*, Docket No. RM14-15-000 (May 23, 2014) [hereinafter CIP-014-1 Petition].

[21] March 7 Order, *supra* note 18, at P 6 (emphasis added). In the March 7 Order, the Commission stated, "[W]e anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System." *Id.* at P 12.

[22] *Id.* at P 8 (emphasis added).

[23] *Id.* at P 9 (emphasis added).

against and mitigate the impact of physical attacks that may compromise the operability or recovery of the identified critical facilities (Requirement R5).

Additionally, the standard addresses the Commission's directives that the standard include: (i) procedures to ensure confidential treatment of sensitive or confidential information; (ii) third-party verification of the identification of critical facilities as well as third-party review of the evaluation of threats and vulnerabilities and the security plans; and (iii) the periodic reevaluation and revision of the identification of critical facilities, the evaluation of threats and vulnerabilities, and the security plans to help ensure their continued effectiveness.[24]

Following a public rulemaking process, the Commission found that Reliability Standard CIP-014-1 satisfied its directives in the March 7 Order and approved the standard as just, reasonable, not unduly discriminatory or preferential, and in the public interest.[25] Subsequently, on July 14, 2015, the Commission approved a revised version of the standard (Reliability Standard CIP-014-2), which, at the Commission's request, included a slight clarification in the wording of the standard.[26]

The Complaint is deficient and should be dismissed because it does not offer any factual evidence in support of its assertion that Reliability Standard CIP-014-2 is inadequate to protect reliability. The Complaint asserts that the standard is "inadequate" because "[t]here is no requirement that an entity's risk assessment or physical security plan be reviewed by anyone with any physical security expertise. There is no regulator determination whatsoever as to the

---

[24] *See id.* at PP 10-11 and CIP-014-1 Petition, *supra* note 20, at 3-4 and Exhibit D (Consideration of Directives).

[25] *Physical Security Reliability Standard*, Order No. 802, 149 FERC ¶ 61,140 at P 18 (2014) [hereinafter Order No. 802], *reh'g denied, Physical Security Reliability Standard,* Order Denying Rehearing, 151 FERC ¶ 61,066 (2015).

[26] In approving CIP-014-1, the Commission directed NERC to address concerns regarding the term "widespread." *See id.* at P 31. NERC developed Reliability Standard CIP-014-2 in accordance with its standard development procedure to address the Commission's directive. NERC's properly noticed and uncontested filing seeking approval of CIP-014-2 was approved by the Commission on July 14, 2015. *N. Am. Elec. Reliability Corp.*, Docket No. RD15-4-000 (July 14, 2015) (delegated letter order).

effectiveness of any entity's physical security plan."[27] The Supplemental Complaint, citing historical information which by its own admission precedes CIP-014-1,[28] further asserts that the standard is not applicable to a large enough number of facilities[29] and contains numerous deficiencies and so-called "loopholes" that must be corrected through specific revisions to the standard.[30]

The assertions in the Complaint and Supplemental Complaint offer hypothetical situations about how an entity could attempt to circumvent the requirements of Reliability Standard CIP-014-2, including by colluding with other entities. The Complaint fails to offer any new information or facts that purport to actually demonstrate the inadequacy of those requirements.[31] Further, the Complaint fails to offer a plausible explanation of how the standard does not require review of risk assessments and physical security plans by entities with the proper expertise to review such documents. However, rather than repeat the justifications for the applicability and each of the individual requirements of the CIP-014 standard here, NERC refers the Commission to the record of Docket Nos. RM14-15-000 and RD15-4-000.

---

[27] Complaint at 1. *See also id.* at 4 ("All the infrastructure owner must do is to have a binder with a bunch of papers labeled 'Physical Security Plan' and have any peer utility they choose review the 'risk assessment,' 'evaluation' and 'security plan(s).'").

[28] Supplemental Complaint at 2.

[29] Supplemental Complaint at 6.

[30] Supplemental Complaint at 6-10.

[31] *See, e.g.*, Supplemental Complaint at 7 ("R2.2 Loophole #1: Many, if not all, peer Transmission Owners would meet the requirement to be a 'verifying entity.' This means that peer Transmission Owners could verify each other's risk assessments. This creates an obvious conflict of interest and could incent Transmission Owners to 'go easy – they are verifying us next week.'"). *See also id.* at 9 ("One acceptable 'unaffiliated third party' under R6.1 is: 'An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.' However, this one member on the review staff may not be the leader or the person writing the 'review.' There is sufficient 'flexibility' to marginalize the role of this 'at least one member' of the review staff who has experience, in this largely paper exercise. There is no requirement that this one member who might have some knowledge perform any type of on-site evaluation. In the end, this loophole makes the qualifications and marching orders of the 'review staff' – especially peer utilities – suspect.").

NERC observes that the assertions in the Complaint and Supplemental Complaint could have been raised in comments submitted during NERC's open and inclusive standard development process,[32] or the Commission's own public rulemaking processes, where they could have been addressed on the record. The failure to do so then does not provide the grounds for a complaint now. Indeed, several of the Complainant's recommendations for changes to CIP-014-2 resemble those raised by the Foundation for Resilient Societies in its request for rehearing, which the Commission ultimately rejected.[33]

While NERC believes that the Commission should dismiss the Complaint for the procedural deficiencies stated above, NERC also believes that the allegations in the Complaint—that Reliability Standard CIP-014-2 is inadequate to protect reliability and that the Commission should direct further changes at this time—are without merit. As NERC stated in its 2019 State of Reliability Report:

> In 2018, as in previous years, there were no reported cyber or physical security incidents on BES facilities that resulted in a loss of load. This is the single most important security measure because it shows that the combined efforts of industry, NERC, the E-ISAC, and government partners have so far been successful in protecting the BPS's reliability.[34]

---

[32] Indeed, NERC notes that its process allows any stakeholder to submit a new request to revise a standard through its standard development process. No such request has been submitted by the Complainant for Reliability Standard CIP-014-2.

[33] *Compare Physical Security Reliability Standard*, Order Denying Rehearing, 151 FERC ¶ 61,066 at PP 11, 16, and 30 (2015) (denying rehearing request based on alleged errors and deficiencies in the standard related to modeling the loss of one facility, CIP-014 applicability, and specific requirements or suggested guidelines for physical security measures) *with* Complaint at 5 (calling for modeling the loss of more than one facility), Complaint at 5 and Supplemental Complaint at 4-6 (calling for additional applicable entities), *and* Supplemental Complaint at 9-10 (calling for specific types of physical security measures to be included in physical security plans). The Complainant is aware of the Commission's action denying the rehearing requested by the Foundation for Resilient Societies. *See* Supplemental Complaint at 4 n.17, n.18, and 6 n.27.

[34] NERC State of Reliability Report at 67 (2019), https://www nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf.

Ensuring the security of the grid has always been a top priority of NERC, and NERC has actively monitored the implementation of Reliability Standard CIP-014-2. NERC committed to its Board of Trustees to review implementation of the standard and to submit reports accordingly.[35] NERC also filed with the Commission a report reviewing whether additional Control Centers should come into scope of Reliability Standard CIP-014-2.[36] Based on the findings of that report, the NERC Critical Infrastructure Protection Committee developed security guidelines to assist entities in protecting certain Control Centers.[37] To the extent that new information or evolving risks indicate the need to revise Reliability Standard CIP-014-2 to ensure its continued effectiveness, NERC should have the opportunity to pursue the appropriate revisions through its open and inclusive standard development process.

B. The Complainant Has Failed to Demonstrate That Enforcement of Reliability Standard CIP-014-2 is Inadequate.

The Complaint and Supplemental Complaint allege that enforcement of CIP-014-2 "seems nonexistent" and claim that utilities have only been cited four times for violations of CIP-014-2.[38] The Complainant requests that the Commission direct NERC to submit to the Commission for approval a compliance and enforcement plan for physical security.[39] The Complainant has failed

---

35 *See*, Order No. 802, *supra* note 25, at PP 44, 70-71.

36 *CIP-014 Report –Security Protection for High Impact Control Centers*, Informational Filing, Docket No. RM15-14-000 (October 2, 2017), https://www nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/CIP-014%20High%20Impact%20Control%20Center%20Report.pdf.

37 NERC CIP Committee, *Security Considerations for High-Impact Control Centers* (December 12, 2018), https://www nerc.com/comm/CIPC_Security_Guidelines_DL/Physical%20Security%20Guideline%20Security%20Considerations%20High%20Impact%20Control%20Centers.pdf.

38 Complaint at 1 and 5-7.

39 *Id.* at 7.

to meet its burden under the Commission's rules, providing speculative arguments and conflating CIP-014-2 with CIP-001-1 and EOP-004-1, which had different reliability and security goals.[40]

Aside from being speculative and unsupported, the Complainant's allegation is not accurate. While the Complaint and Supplemental Complaint identify three Notices of Penalty that involved a total of four CIP-014-2 violations,[41] NERC has publicly posted an additional three moderate risk instances of CIP-014 noncompliance resolved through the Find, Fix, Track and Report ("FFT") disposition method,[42] and nine minimal risk CIP-014 noncompliance resolved through the Compliance Exception disposition method.[43] As of January 31, 2020, NERC had publicly reported 16 instances of CIP-014 noncompliance.

NERC has received additional instances of CIP-014 noncompliance that have not been resolved yet. Of all reported CIP-014 noncompliance, Regional Entities identified approximately two-thirds via compliance audits they conducted of registered entities, and registered entities self-

---

[40] *Compare* purpose statement of CIP-014-2 ("To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection") *with* purpose statement of CIP-001-1 ("Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies") *and* purpose statement of EOP-004-1 ("Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future"). CIP-014-2 is intended to identify and protect critical infrastructure, while CIP-001-1 and EOP-004-1 are intended to result in the reporting and study of disturbances or unusual occurrences affecting the Bulk Electric System.

[41] *See* NP17-29-000 (September 28, 2017) (involving two CIP-014-2 noncompliance resolved in a Spreadsheet Notice of Penalty), NP18-14-000 (May 31, 2018) (involving one CIP-014-2 noncompliance resolved in a full Notice of Penalty), and NP19-4-000 (January 25, 2019) (involving one CIP-014-2 noncompliance resolved in a full Notice of Penalty).

[42] FFTs posted on December 31, 2019 (involving CIP-014-2 R4, R5, and R6), available at https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_A-2_FinalPosted_FFT_Summary_01-30-2020.pdf.

[43] Compliance Exceptions posted on May 31, 2016, May 31, 2017, July 31, 2017, August 31, 2017, October 31, 2017, February 28, 2019, and March 28, 2019 (involving CIP-014 R1, R4, R5, and R6), available at https://www nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/A-2_Public_CIP_FinalPosted_CE_Summary_01-31-2019.xlsx (pre-2019 issues only) and https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_A-2_FinalPosted_CE_Summary_01-30-2020.pdf (2019 issues).

reported the remaining noncompliance. This demonstrates two important points: (1) Regional Entities are looking at CIP-014 when conducting compliance monitoring engagements of registered entities and finding deficiencies that registered entities will need to correct as part of their mitigation efforts and steps to prevent recurrence,[44] and (2) registered entities are also examining their compliance with the CIP-014 Reliability Standard and notifying their respective Regional Entities of self-identified deficiencies and actions they are taking to return to compliance and prevent recurrence.[45] Pursuant to the Commission-approved NERC Rules of Procedure, open enforcement actions remain non-public until resolution, and additional details about these noncompliance will remain confidential until they are resolved.[46]

Outside of the enforcement context, NERC and the Regional Entities have invested significant effort to ensure that registered entities are taking their obligations under CIP-014 seriously. NERC and the Regional Entities conducted a self-certification in 2016 involving all Transmission Owners related to CIP-014-2, Requirements R1 through R3 to determine the number of registered entities to which CIP-014-2 applied, whether they conducted a risk assessment and

---

[44] *See* NERC Rules of Procedure, *supra* note 8, Section 403(8)(10.5) ("A Bulk Power System owner, operator, or user found in noncompliance with a Reliability Standard shall submit a Mitigation Plan with a timeline addressing how the noncompliance will be corrected, unless an enforcement process is used that does not require a Mitigation Plan. The Regional Entity Compliance Staff shall review and accept the Mitigation Plan in accordance with Appendix 4C") and Appendix 4C, Section 6 (requiring registered entities to file either a proposed Mitigation Plan to correct the violation or a description of how the violation has been mitigated, and laying out the various requirements for Mitigation Plans).

[45] *See id.*, Appendix 4C, Section 3.5 (noting that "Self-Reports are encouraged at a time a Registered Entity becomes aware (i) that is has, or may have violated a Reliability Standard…" and that Self-Reports "may include the actions that have been taken or will be taken to resolve the violation.").

[46] *See id.*, Section 9.3.1 ("Information or data generated or received pursuant to Compliance Program activities, including a hearing process, shall be treated in a confidential manner pursuant to the provisions of Section 1500 of the NERC Rules of Procedure."); Section 401(10) (noting that NERC "will treat all Possible and Alleged Violations of Reliability Standards and matters related to a Compliance Monitoring and Enforcement Program process… as confidential in accordance with Section 1500."); and Section 1506 (permitting disclosure of a violation "at the point when the matter is filed with an Applicable Governmental Authority as a Notice of Penalty, the 'violator' admits the violation, or the alleged violator and NERC or the Regional Entity reach a settlement regarding the violation.").

verification or notification activities as required, whether they identified any critical Transmission stations or substations, and the number of such critical facilities.[47] To assist registered entities in completing the self-certification, NERC conducted a CIP-014-2 self-certification webinar that was attended by over 200 participants, and the ERO Enterprise conducted outreach through on-site engagements with 19 registered entities in six Regional Entity footprints.[48]

In the 2017 Annual CMEP Implementation Plan, NERC and the Regional Entities reported that they had begun engaging registered entities "through a variety of outreach activities and coordinated site visits to discuss and understand their implementation of CIP-014-2" and that initial observations indicated industry was "making progress toward effective implementation of and compliance with CIP-014-2."[49]

The ERO Enterprise has included CIP-014-2 as an area of focus in its Annual CMEP Implementation Plans from 2016-2019, as part of two different risk elements: "Extreme Physical Events" (2016-2018) and "Spare Equipment with Extended Lead Time" (2019).[50] While not identified as an area of focus in the 2020 CMEP Implementation Plan, the risk of physical threats

---

47 NERC, *2016 ERO Enterprise CMEP Implementation Plan*, Version 2.5 (July 2016), at 16, available at https://www.nerc.com/pa/comp/Resources/ResourcesDL/2016%20CMEP%20IP_v_2%205_071116_POSTED.pdf.

48 NERC, *2016 ERO Enterprise CMEP Annual Report* (February 2017) at 18-19, available at https://www.nerc.com/pa/comp/CE/ReportsDL/2016%20Annual%20CMEP%20Report.pdf.

49 NERC, *2017 ERO Enterprise CMEP Implementation Plan*, Version 2.5 (May 2017) at 16, available at https://www nerc.com/pa/comp/Reliability%20Assurance%20Initiative/2017%20ERO%20CMEP%20Implementation%20Plan.pdf.

50 *2016 CMEP Implementation Plan*, *supra* note 47, (CIP-014-2 discussions on pages 3, 11, and 16), *2017 CMEP Implementation Plan*, s*upra* note 49, (CIP-014-2 discussions on pages 2, 10, and 15-16, noting that FERC staff and NERC staff coordinated in support of joint visits to registered entities in 2016 to evaluate progress on implementation of CIP-014-2), NERC, *2018 ERO Enterprise CMEP Implementation Plan*, Version 2.1 (May 2018), available at https://www.nerc.com/pa/comp/Resources/ResourcesDL/2018_ERO_CMEP_Implementation%20Plan_V2.1_May_2018.pdf (CIP-014-2 discussions on pages 2, and 10-11), and *2019 ERO Enterprise CMEP Implementation Plan*, Version 2.1 (November 2018), available at https://www.nerc.com/pa/comp/Resources/ResourcesDL/2019_ERO_CMEP_Implementation%20Plan_V2%20November%202018.pdf (CIP-014-2 discussions on pages 12-13).

or breaches was part of the risk element of "Loss of Major Transmission Equipment with Extended Lead Times."[51] The Annual CMEP Implementation Plans identify risk elements that the Regional Entities will consider as part of their compliance monitoring activities for registered entities in the coming year and include specific Standards and Requirements as areas of focus for each identified risk element. As noted above, most of the identified noncompliance with CIP-014 to date has been found by Regional Entities conducting compliance audits.

In addition, the ERO Enterprise has endorsed three different Implementation Guidance documents for CIP-014-2, which provide examples for registered entities to consider when implementing a Reliability Standard.[52] The three ERO Enterprise-endorsed CIP-014 Implementation Guidance documents address CIP-014-2 R1 (initial and subsequent risk assessments),[53] CIP-014-2 R4 (evaluation of potential threats and vulnerabilities of a physical

[51] NERC, *2020 ERO Enterprise CMEP Implementation Plan*, Version 2.0 (November 2019), available at https://www nerc.com/pa/comp/CAOneStopShop/2020_ERO_CMEP_Implementation%20Plan.pdf (physical security breaches and threats discussed on page 9).

[52] ERO Enterprise-endorsed Implementation Guidance is available at https://www nerc.com/pa/comp/guidance/Pages/default.aspx. The policy governing the ERO Enterprise's endorsement of Implementation Guidance was approved by the NERC Board of Trustees on November 5, 2015 and is available at https://www nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf.

[53] *North American Transmission Forum CIP-014-2 Requirement R1 Guideline* (2017), available at https://www nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-014-2%20R1%20Guideline%20(NATF).pdf (providing guidance to Transmission Owners on possible ways to perform an initial and subsequent risk assessments to identify the Transmission station(s), Transmission substation(s) that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection).

attack),[54] and CIP-014-2 R5 (developing and implemental physical security plan(s)).[55] These documents provide registered entities with vetted examples of possible approaches to demonstrate the reliability and security goals associated with the CIP-014 Reliability Standard and its Requirements.

Finally, NERC notes that the Complainant's allegation that enforcement of CIP-014-2 seems nonexistent based on the low number of publicly posted noncompliance cuts both ways. Rather than demonstrate that enforcement is nonexistent, the small number of CIP-014-2 noncompliance, as well as the more administrative nature of the CIP-014-2 noncompliance publicly posted to date, could instead demonstrate that (1) registered entities have taken their obligations under CIP-014-2 seriously and implemented sufficient controls to prevent or quickly detect noncompliance, and (2) the outreach efforts taken by the ERO Enterprise have been effective at preparing registered entities to demonstrate compliance with the Reliability Standard. The Complainant's logic results in a Catch-22: low levels of CIP-014-2 violations mean that the Standard is inadequate or not being adequately enforced by the ERO Enterprise, while high levels of violations would mean that registered entities are not taking their physical security obligations seriously.

---

[54] *North American Transmission Forum Practices Document for NERC Reliability Standard CIP-014-2 Requirement R4* (2018), available at https://www nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-014-2%20R4%20Evaluating%20Potential%20Physical%20Security%20Attack.pdf (providing guidance to Transmission Owners and Transmission Operators on possible ways to perform an evaluation of potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)).

[55] *North American Transmission Forum Practices Document for NERC Reliability Standard CIP-014-2 Requirement R5* (2018), available at https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-014-2_R5_Developing_and_Implementing_Physical_Security_Plans_(NATF).pdf (providing guidance to Transmission Owners and Transmission Operators on possible ways to develop and implement physical security plan(s) to protect their respective Transmission station(s), Transmission substation(s), and primary control center(s)).

NERC believes that registered entities have a clear interest in ensuring the physical security of their systems and the BPS as a whole. As described above, the ERO Enterprise has conducted outreach to ensure that registered entities were prepared for CIP-014-2, monitors registered entities' compliance with the Reliability Standard, takes appropriate risk-based enforcement steps when noncompliance is discovered, and requires registered entities to mitigate and prevent recurrence of such noncompliance.

C. The Commission is Already Evaluating the Adequacy of Registered Entities' Compliance with Reliability Standard CIP-014-2.

The Complainant argues that FERC should evaluate registered entities' physical security programs to determine if they are effective.[56] While this recommendation does not directly affect NERC, NERC notes that the Commission addressed this issue in Order 802, stating that it would "focus its resources on carrying out compliance and enforcement activities to ensure that critical facilities are identified under Requirement R1."[57] The Commission further noted that it expected Commission staff to:

> audit a representative number of applicable entities to ensure compliance with Reliability Standard CIP-014-1. Depending on the audit findings, the Commission will determine if there is a need for any further action by the Commission including, but not limited to, directing NERC to develop modifications to Reliability Standard CIP-014-1 to provide greater specificity to the methodology for determining critical facilities.[58]

In March 2018, the Congressional Research Service reported that, as of November 2, 2017, the Commission had:

---

56 Complaint at 7.
57 Order 802, *supra* note 25, at P 44.
58 *Id.*

> completed two audits of critical assets identified by covered entities (R1) and was in the process of conducting a third. These audits have involved technical review of utility regulatory documents by FERC engineers.[59]

Commission staff have already conducted evaluations of registered entities' compliance with CIP-014-2, and Complainant provides no explanation of what additional benefit would be achieved by coordinating such efforts with other departments within the federal government, the National Guard, or state public utility commissions.

V. CONCLUSION

WHEREFORE, for the reasons stated above, NERC respectfully requests that the Commission grant this motion to intervene, accept the comments herein, and dismiss the Complaint.

[59] Congressional Research Service, "NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?" at 8 (2018), available at https://crsreports.congress.gov/product/pdf/R/R45135.

Respectfully submitted,

/s/ James McGrane

James McGrane
Senior Counsel
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Lauren 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
james.mcgrane@nerc.net
ed.kichline@nerc.net
lauren.perotti@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: March 2, 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 2nd day of March, 2020.

/s/ James McGrane
James McGrane
Counsel for the North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards under the NERC Standards Efficiency Review	**)** **)** **)** **)**	**Docket Nos. RM19-16-000** **RM19-17-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") hereby provides comments on the Notice of Proposed Rulemaking ("NOPR") regarding NERC's proposal to retire requirements in Reliability Standards issued by the Federal Energy Regulatory Commission ("FERC" or "Commission") in this proceeding on January 23, 2020.[1] NERC provides these comments as the Commission-certified electric reliability organization ("ERO") responsible for the development and enforcement of mandatory Reliability Standards, including the proposals referenced in the NOPR.[2]

In the NOPR, the Commission proposes to approve 74 of the 77 total requirement retirement proposals proposed by NERC in two petitions filed with the Commission on June 7, 2019, including: (i) the retirement of ten currently effective Reliability Standards in their entirety;[3]

---

[1] Notice of Proposed Rulemaking, *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards under the NERC Standards Efficiency Review*, 170 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] The Commission proposes to approve the retirement of 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, and MOD-030-3 as proposed by NERC.

and (ii) proposed Reliability Standards INT-006-5, INT-009-3, IRO-002-7, PRC-004-6, and TOP-001-5, in which individual requirements of the currently effective standards are proposed to be retired. The Commission also proposes to approve the associated Violation Risk Factors, Violation Severity Levels, implementation plan, and effective dates as proposed by NERC.[4] The Commission seeks additional information regarding the proposed retirement of Requirements R7 and R8 in proposed Reliability Standard FAC-008-4.[5] The Commission also proposes to remand proposed Reliability Standard VAR-001-6 to retain Requirement R2.[6]

NERC supports the Commission's proposal to approve NERC's retirement proposals. In these comments, NERC offers additional information in support of proposed Reliability Standard FAC-008-4 as requested by the Commission. As discussed in these comments, NERC respectfully requests that the Commission defer action on its NOPR proposal to remand proposed Reliability Standard VAR-001-6 until after the NERC Board of Trustees has had the opportunity to consider the Commission's concerns at its May 14, 2020 meeting and determine whether to take further action with respect to the proposed standard.

I. BACKGROUND

A. The Standards Efficiency Review Petitions

On June 7, 2019, NERC submitted two petitions originating from work under the first phase of the NERC Standards Efficiency Review. This initiative, which began in 2017, reviewed the body of NERC Reliability Standards to identify those Reliability Standards and requirements that are administrative in nature or relate expressly to commercial or business practices, are redundant to other Reliability Standards, or provide little to no benefit to reliability. NERC

4 NOPR, *supra*, at P 1.
5 *Id.* at P 33.
6 *Id.* at PP 38-39.

identified 77 Reliability Standard requirements for retirement and one proposed standard for withdrawal. NERC's filings consisted of the following. First, NERC filed a petition to retire ten currently effective standards in their entirety and approve four revised Reliability Standards in which individual requirements are retired, involving the FAC, INT, MOD, and PRC Reliability Standard families (retirement of 73 requirements).[7] Second, NERC filed a petition to approve the following three revised Reliability Standards in which individual retirements are retired: IRO-002-7, TOP-001-5, and VAR-001-6 (retirement of 4 requirements).[8]

B. The NOPR

On January 23, 2020, the Commission issued the NOPR. In the NOPR, the Commission proposes to approve 74 of the 77 Reliability Standard requirements requested for retirement by NERC, including all of the proposals involving the INT, IRO, PRC, MOD, and TOP Reliability Standard families.[9] The Commission, however, expressed concern with the remaining three retirement proposals.

With respect to the retirement of Requirements R7 and R8 in proposed Reliability Standard FAC-008-4, the Commission states that it agrees with NERC that other Reliability Standards overlap with certain elements of Requirements R7 and R8. The Commission, however, expresses concern that these requirements "do not appear to be entirely redundant of the other Reliability

---

[7] *Petition of NERC for Approval of Revised and Retired Reliability Standards under the NERC Standards Efficiency Review*, Docket No. RM19-17-000 (June 7, 2019) [hereinafter the FAC, INT, MOD, and PRC Petition]. This petition proposed to retire Reliability Standards 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, and MOD-030-3, and proposed revised Reliability Standards FAC-008-4, INT-006-5, INT-009-3, and PRC-004-6. Concurrently with the filing of this petition, NERC submitted a notice to withdraw its 2014 petition for approval of MOD-001-2, which was then pending Commission action. *Notice of Withdrawal of NERC for Proposed Reliability Standard MOD-001-2*, Docket No. RM14-7-000 (June 7, 2019).

[8] *Petition of NERC for Approval of Reliability Standards IRO-002-7, TOP-001-5, and VAR-001-6 Developed under the NERC Standards Efficiency Review*, Docket No. RM19-16-000 (June 7, 2019) [hereinafter the IRO, TOP, and VAR Petition].

[9] NOPR, *supra*, at PP 25-27.

Standards cited by NERC."[10] Specifically, the Commission expresses concern that Reliability Standards MOD-032-1, IRO-010-2, and TOP-003-3 "do not require the provision of facility ratings to transmission owners" and if the retirements were approved, reliability could be impacted "since these requirements ensure that all transmission owners have accurate facility-related information in the models that they use to plan and operate the bulk electric system."[11] The Commission also states the cited Reliability Standards do not address Reliability Standard FAC-008-3 Requirement R8 Part 8.1.2, relating to the identity of the next most limiting equipment of a requested facility, or Part 8.2.2, requiring the identification and thermal rating of the existing next most limiting equipment of facilities with a thermal rating that limits the use of that facility by causing either an Interconnection Reliability Operating Limit, a limitation of Total Transfer Capability, an impediment to generator deliverability, or an impediment to service to a major load center.[12] The Commission states that its final determination on the retirement of these two requirements will be based on comments received from NERC and others.[13]

In the NOPR, the Commission proposes to remand Reliability Standard VAR-001-6 because "it is the only requirement that explicitly requires transmission operators to schedule reactive resources."[14] The Commission expresses disagreement that Reliability Standard VAR-001-5 Requirement R2 is duplicative of other existing Reliability Standard requirements and states, "While Reliability Standards TOP-001-4 and TOP-002-4 address situations involving the possible need to schedule reactive resources, they are not adequate substitutes for the explicit obligation in Requirement R2 of Reliability Standard VAR-001-5 requiring transmission operators to schedule

10 *Id.* at P 33.
11 *Id.* at P 31.
12 *Id.* at P 32.
13 *Id.* at P 33.
14 *Id.* at P 38.

enough reactive resources to regulate voltage levels under all system conditions."[15] The Commission further states, "Reliability Standards TOP-001-4 and TOP-002-4 do not require the transmission operator to implement mitigation plans: instead, the transmission operator need only analyze and develop a plan to address a potential System Operating Limit."[16] The Commission therefore proposes to remand proposed Reliability Standard VAR-001-6 in order to retain Requirement R2 of the currently effective standard.[17]

NERC's comments on these proposals is provided in the following section.

II. COMMENTS

NERC supports the Commission's proposal to approve 74 of the 77 Reliability Standard requirements requested for retirement by NERC, including all of the proposals involving the INT, IRO, PRC, MOD, and TOP Reliability Standard families. As the Commission states, the proposed retirements will enhance reliability by allowing entities to focus their resources on those Reliability Standard requirements that more effectively promote the reliable operation and planning of the Bulk-Power System. Further, the proposed retirements will improve the efficiency of NERC's Reliability Standards program by reducing duplicative or otherwise unnecessary regulatory burdens.[18] NERC submits that the Commission should also approve proposed Reliability Standard

15 *Id.* at P 39.
16 *Id.* at P 40.
17 *Id.* at PP 34-41.
18 *See id.* at P 2.

FAC-008-4, in which Requirements R7 and R8 of the currently effective standard are proposed to be retired. NERC's comments on the specific issues raised in the NOPR are provided below.

A. NERC Supports the NOPR Proposal to Approve Retirement of Reliability Standard Requirements

As noted above, NERC supports the Commission's proposal to approve the 74 retirements identified in the NOPR and encourages the Commission to approve these retirements in a final rule issued in this proceeding.

While not discussed specifically in the NOPR, NERC notes that there are additional reasons that would support the retirement of Reliability Standard MOD-020-0 – Providing Interruptible Demands and Direct Control Load Management Data to System Operators and Reliability Coordinators. In NERC's FAC, INT, MOD, and PRC Petition, NERC stated that the standard should be retired on the basis that it provides little, if any, benefit to reliability and, to the extent that entities do find the specified data to be useful as a longer-term resource, it may be obtained through other mechanisms, including NERC's Demand Response Availability System ("DADS").[19] In these comments, NERC adds that Reliability Standard MOD-031-2 – Demand and Energy Data also provides a means for obtaining demand response information.

The purpose of Reliability Standard MOD-031-2 is to provide authority for applicable entities to collect Demand, energy, and related data to support reliability studies and assessments and to enumerate the responsibilities and obligations of requestors and respondents to that data. Requirement R1 provides that a Planning Coordinator and Balancing Authority identifying a need for the collection of Demand Side Management data shall develop and issue data requests to Transmission Planners, Balancing Authorities, Load Serving Entities, and Distribution Providers for load data including monthly and annual peak hour controllable and dispatchable Demand Side

[19] FAC. INT, MOD, and PRC Petition, *supra*, at 23-24.

Management under the control or supervision of the System Operator in megawatts for the prior calendar year (Requirement Part R1.3.4)[20] and the Demand and energy effects of controllable and dispatchable Demand Side Management under the control or supervision of the System Operator (Requirement Part R1.5.2). Requirement R4 provides that any applicable entity shall provide such data in response to a request from a Planning Coordinator, Balancing Authority, Transmission Planner, or Resource Planner with a demonstrated need for the data. NERC notes that the Reliability Coordinator has the authority to obtain data necessary for planning and operations using its authority under Reliability Standard IRO-010-2 – Reliability Coordinator Data Specification and Collection.

For the reasons provided in NERC's petition and in these comments, NERC supports the Commission's NOPR proposal to approve the retirement of 74 Reliability Standard requirements, including the retirement of Reliability Standard MOD-020-0 in its entirety.

B. Reliability Standard FAC-008-3 Requirements R7 and R8 are Not Needed for Reliability and May be Retired in Proposed FAC-008-4

In the NOPR, the Commission states that FAC-008-3 Requirement R7 and R8 may not be fully redundant with the Reliability Standards cited by NERC in its petition, and it seeks additional information regarding the proposed retirement of these requirements in proposed FAC-008-4.[21]

With respect to the Commission's concern that eliminating the mandatory exchange of facility rating-related information with Transmission Owners could "impact reliability since these requirements ensure that all transmission owners have accurate facility-related information in the

[20] The standard provides that three values shall be reported for each hour: 1) the committed megawatts (the amount under control or supervision), 2) the dispatched megawatts (the amount, if any, activated for use by the System Operator), and 3) the realized megawatts (the amount of actual demand reduction).

[21] *See* FAC, INT, MOD, and PRC Petition, *supra*, at 27-28. These Reliability Standards are MOD-032-1, IRO-010-2, and TOP-003-3.

models that they use to plan and operate the bulk electric system,"[22] NERC responds as follows. Under NERC's Reliability Standards program, the Transmission Owner, defined in the NERC Glossary as "[t]he entity that owns and maintains transmission Facilities,"[23] is not the functional entity directly responsible for complying with Reliability Standards for planning and operating the Bulk-Power System. NERC has a mechanism in place to register Transmission Owners as Transmission Planners or Transmission Operators if they are in fact planning or operating the Bulk-Power System. The exchange of facility ratings information with these functional entities is addressed in Reliability Standards MOD-032-1 and TOP-003-3, as stated in NERC's petition. NERC therefore maintains that there would be no reliability gap from eliminating the mandatory exchange of facility rating-related information with Transmission Owners in proposed FAC-008-4.

With respect to the Commission's concern in the NOPR that Reliability Standards MOD-032-1, IRO-010-2, and TOP-003-3 do not appear to address Reliability Standard FAC-008-3 Requirement R8 Part 8.1.2, relating to the identity of the next most limiting equipment of a requested facility, or Part 8.2, requiring the identification and thermal rating of the existing next most limiting equipment of facilities with a thermal rating that limits the use of that facility,[24] NERC responds as follows. The provision of such information by the Transmission Owner and Generator Owner to the Planning Coordinator and Transmission Planner is addressed by Reliability Standard MOD-032-1 Attachment 1 Data Reporting Requirements. Attachment 1 contains a "catch-all" provision that requires the Transmission Owner and Generator Owner to

[22] *See* NOPR, *supra*, at P 31.

[23] Glossary of Terms Used in NERC Reliability Standards, https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[24] NOPR, *supra*, at P 32.

provide "[o]ther information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes."[25] This information would include the data that is now explicitly enumerated under FAC-008-3 Requirement R8 Parts 8.1.2 and 8.2. The provision of this data to the Reliability Coordinator and Transmission Operator is addressed under the data specification requirements in Reliability Standards IRO-010-2 and TOP-003-3, respectively.

In summary, Reliability Standards MOD-032-1, IRO-010-2, and TOP-003-3 provide the entities responsible for the reliable modeling, planning, and operation of the BPS with the authority to obtain the information they need from Generator Owners and Transmission Owners to complete their reliability tasks, which may include next most limiting equipment information. Now that these broader data specification standards are in place, NERC has identified no reliability need to maintain additional requirements expressly requiring the provision of this data in the FAC-008 standard. NERC therefore respectfully requests that the Commission approve proposed Reliability Standard FAC-008-4 in which these requirements are proposed to be retired.

C. NERC Requests that the Commission Defer Action on its Proposal to Remand Reliability Standard VAR-001-6

In the NOPR, the Commission proposes to remand proposed Reliability Standard VAR-001-6 in order to retain Requirement R2. While NERC maintains that the retirement of Requirement R2 would not pose an unacceptable risk to the BPS for the reasons stated in its petition,[26] NERC acknowledges the Commission's concerns as stated in the NOPR. NERC respectfully requests that the Commission defer action on this NOPR proposal until the NERC Board of Trustees has had the opportunity to consider whether to take further action with respect to the proposed standard at its May 14, 2020 meeting. NERC would inform the Commission of the

[25] *See* MOD-032-1 Attachment 1, steady-state column, item 9.
[26] IRO, TOP, VAR Petition at 18.

outcome through the timely submission of one or more appropriate filings so as to not unduly delay the issuance of a final rule in this proceeding.

III. CONCLUSION

NERC respectfully requests that the Commission accept these comments for consideration.

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

Date: April 6, 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 6th day of April, 2020.

/s/ Lauren A. Perotti

Lauren A. Perotti

Counsel for the North American Electric Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 30, 2020

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: NERC Standards Report, Status and Timetable for Addressing Regulatory Directives
Docket No. RR09-6-003

Dear Secretary Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits the 2020 NERC Standards Report, Status and Timetable for Addressing Regulatory Directives (the "Directives Report") in accordance with Section 321.6 of the NERC Rules of Procedure ("ROP").[1] This annual report summarizes the progress made and plans for addressing the Reliability Standard-related directives issued by applicable governmental authorities.

Section 321.6 of NERC's ROP requires NERC, on or before March 31 of each year, to file a report with applicable governmental authorities on the status and timetable for addressing each outstanding regulatory directive.

As discussed in the attached Directives Report, since NERC's 2019 annual directives report filed on March 29, 2019, the Commission has issued three new directives related to Reliability Standards. In that time, NERC filed petitions with the Commission addressing eight directives.[2] Currently, there are nine outstanding directives, four of which NERC is addressing through standards development projects. The other outstanding directives are not related to Reliability Standards development (i.e., the directives relate to data gathering, registration, or the performance of research/studies) and are being addressed through other mechanisms.[3]

The 2020-2022 Reliability Standards Development Plan ("RSDP") provides a plan to address the remainder of the standard-related directives. NERC's annual RSDP establishes priorities related to Reliability Standards to help ensure that those issues that most directly impact Bulk-Power System reliability are addressed first. Directives to create new or modify existing Reliability Standards are assigned to existing or future

[1] The Federal Energy Regulatory Commission ("FERC" or "Commission") approved Rule 321 on March 17, 2011 in the above captioned docket. *N. Am. Elec. Reliability Corp., Order on Compliance Filing*, 134 FERC ¶ 61,216 (2011).
[2] *See* Directives Report at Chapter 2, Table 1 for a list of the directives that were addressed since March 29, 2019.
[3] *See id.* at Chapter 2, Table 2 for a list of outstanding directives and status.

development projects that are prioritized by the NERC Standards Committee and reflected in the RSDP. The 2020-2022 RSDP was filed with the Commission on December 13, 2019.[4]

Please contact me if you have questions or need additional information.

Respectfully submitted,

/s/ Lauren A. Perotti
Lauren A. Perotti
Senior Counsel
North American Electric Reliability Corporation
1325 G St., NW, Suite 600
Washington, DC 20005
202-400-3000
lauren.perotti@nerc.net

Counsel to the North American Electric Reliability Corporation

Enclosure:

2020 NERC Standards Report, Status and Timetable for Addressing Regulatory Directives

[4] NERC's 2020-2022 RSDP is accessible at the following link: https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/2020%20RSDP%20FERC%20Filing.pdf.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Standards Report

Status and Timetable for Processing Regulatory Directives

March 30, 2020

RELIABILITY | RESILIENCE | SECURITY






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

Table of Contents

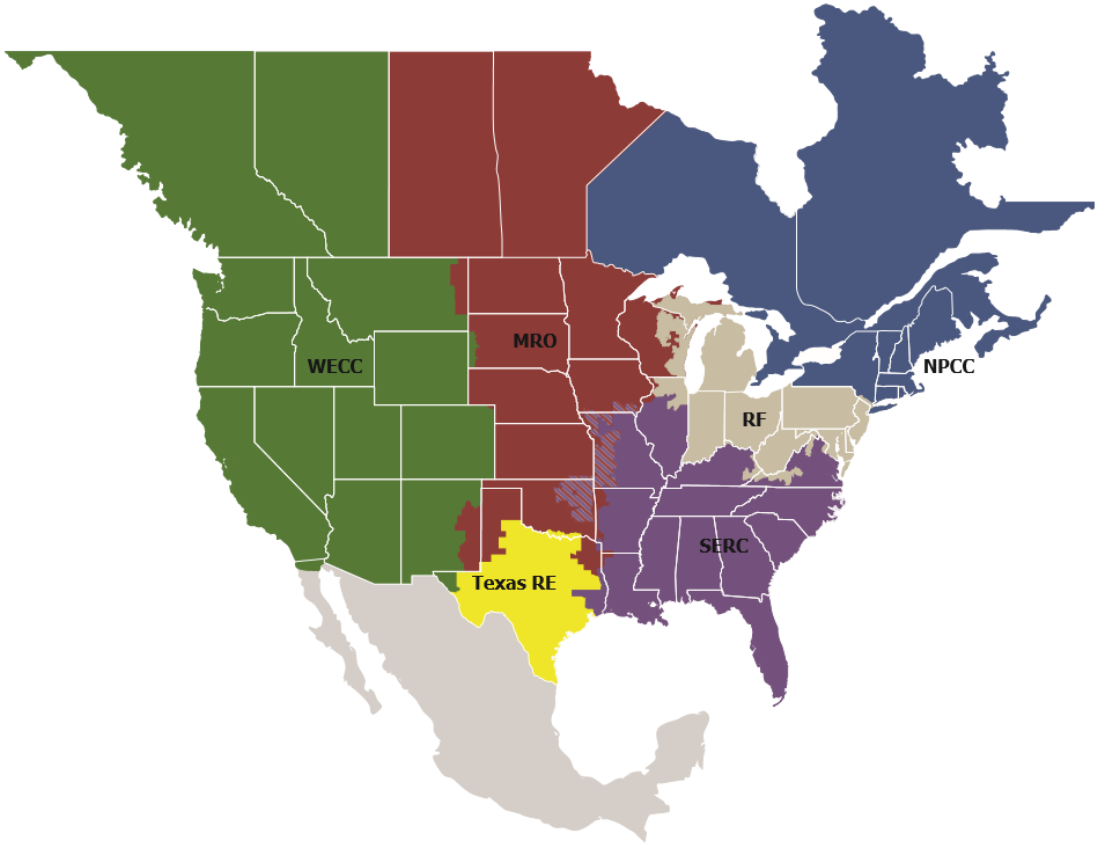
Preface iii
Introduction iv
Background iv
Chapter 1 : Completed Directives 1
Chapter 2 : Outstanding Directives 4
Chapter 3 : Conclusion 7

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk-power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

In accordance with Section 321.6 of the North American Electric Reliability Corporation ("NERC") Rules of Procedure ("ROP"),[1] this report provides an update on the status and timetable for addressing outstanding directives issued by the Federal Energy Regulatory Commission ("FERC" or "Commission") related to Reliability Standards or issued in orders approving or related to Reliability Standards.[2]

As discussed below, since NERC's 2019 annual directives report filed on March 29, 2019, the Commission issued three new directives related to Reliability Standards. In that time, NERC filed petitions or reports with the Commission addressing eight directives.[3] Currently, there are nine outstanding directives, four of which NERC is addressing through existing standards development projects. The other outstanding directives are not related to Reliability Standards development (i.e., the directives relate to data gathering, registration, or the performance of research/studies) and are being addressed through other mechanisms.

NERC's 2020-2022 Reliability Standards Development Plan ("RSDP") provides a plan to address the outstanding Reliability Standard-related directives. NERC's annual RSDP establishes priorities related to Reliability Standards to help ensure that those issues that most directly impact Bulk-Power System reliability are addressed first. Directives to create new or modify existing Reliability Standards are assigned to existing or future development projects that are prioritized by the NERC Standards Committee and reflected in the RSDP. The 2020-2022 RSDP was filed with the Commission on December 13, 2019.[4]

[1] Section 321.6 of NERC's ROP requires NERC, on or before March 31 of each year, to file a report with applicable governmental authorities on the status and timetable for addressing each outstanding regulatory directive.

[2] This report includes both Reliability Standard-related directives and non-Reliability Standard-related directives issued in orders approving or related to Reliability Standards (i.e., directives that pertain to information or data collection as opposed to the development of new or modified Reliability Standards). This report does not include other directives issued by the Commission, such as those issued in orders relating to revisions to the NERC Rules of Procedure or in orders accepting NERC's five year performance assessment filings.

[3] See *infra* Chapter 1, Table 1 for a list of the directives that were addressed since March 29, 2019.

[4] NERC's 2020-2022 RSDP was filed in Docket Nos. RM05-17-000, RM05-25-000, and RM06-16-000 and is available on NERC's website at: https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/2020%20RSDP%20FERC%20Filing.pdf.

Chapter 1: Completed Directives

The tables below contain a status update on the FERC directives. Table 1 contains a complete list of the directives NERC addressed since the 2019 directives report. Table 2 in the next chapter provide a list of the outstanding directives and an update on NERC's plans to address those directives.

Table 1: Directives Addressed since March 30, 2019

Directive Summary	Order No. & Para.	Action Taken	Project Name	Filing Date
S-Ref 10917: "[S]hould NERC make changes to Table 1 [in BAL-003-1.1 Attachment A] based upon NERC's Procedure document, the Commission directs NERC to submit an informational notice describing the basis for the changes at least 30 days in advance of the effective date of any such changes."	Order No. 794 ¶ 100	NERC developed BAL-003-2.	Project 2017-01 Modifications to BAL-003-1.1	12/19/2019
S-Ref 10955: "We further direct NERC to study and submit a report to the Commission with findings regarding reliability risks associated with most severe single contingency exceedances that do not result in energy emergencies."	Order No. 835 ¶ 23	Report was created and filed.	n/a	1/2/2020
S-Ref 10954: ¶ 23: "We also direct NERC to collect and report on data pertaining to the occurrence of Balancing Contingency Events that trigger resets of the 90-minute Contingency Reserve Restoration Period under Requirement R3." | ¶ 46: "[T]he Commission directs NERC to collect and report data pertaining to: (1) additional megawatt losses following Reportable Balancing Contingency Events during the Contingency Reserve Restoration Period; and (2) the time periods for contingency reserve restoration under Requirement R3 and the number of resets of the 90-minute restoration period, and submit a report to the Commission two years following the first day of implementation of Requirement R3. After NERC reports on the data in a	Order No. 835 ¶ 23, 46	Report was created and filed.	n/a	1/2/2020

compliance filing, the Commission will consider what further action, if any, to take."				
"[We] direct NERC to develop and submit modifications to Reliability Standard TPL-007-2 to require the development and completion of corrective action plans to mitigate assessed supplemental GMD event vulnerabilities... The Commission… directs NERC to submit the modified Reliability Standard for approval within 12 months from the effective date of Reliability Standard TPL-007-2."	Order No. 851 ¶ 4, 29	Standard was modified.	Project 2019-01 Modifications to TPL-007-3	2/7/2020 Approved by FERC 3/19/2020
"[We] direct that NERC develop further modifications to Reliability Standard TPL-007-2, Requirement R7.4... [W]e direct NERC to develop a timely and efficient process, consistent with the Commission's guidance in Order No. 830, to consider time extension requests [for completion of Corrective Action Plan activities] on a case-by-case basis."	Order No. 851 ¶ 30	Standard was modified.	Project 2019-01 Modifications to TPL-007-3	2/7/2020 Approved by FERC 3/19/2020
"Accordingly, we accept NERC's commitment to evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the cybersecurity supply chain risks study directed by the BOT. The Commission further directs NERC to file the BOT-directed final report with the Commission upon its completion."	Order No. 850 ¶ 31	Report was created and filed.	n/a	5/28/2019
"We adopt the NOPR proposal and, pursuant to section 215(d)(5) of the FPA, direct that NERC develop modifications to Reliability Standard CIP-003-7 to address our concern and ensure that responsible entities implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices. NERC could satisfactorily address the identified concern, for example, by modifying Section 5 of Attachment 1 to CIP-003-7 to clarify that responsible entities must implement controls to mitigate the risk of malicious code that could result from the use of third-party transient	Order No. 843 ¶ 37	Standard was modified.	Project 2016-02 Modifications to CIP Standards	5/21/2019 Approved by FERC 7/31/2019

electronic devices." | "Therefore, pursuant to FPA section 215(d)(5), we direct NERC to develop and submit modifications to Reliability Standard CIP-003-7 to include an explicit requirement that responsible entities implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices."				
"NERC is directed to make an informational filing for Project 2016-02 and Project 2019-02 within 30 days of the date of issuance of this order."	170 FERC ¶ 61,109 ¶ 5	Filing was created and filed.	Project 2016-02 Modifications to CIP Standards Project 2019-02 BES Cyber System Information Access Management	3/19/2020

Chapter 2: Outstanding Directives

Table 2 below shows the currently outstanding directives from FERC.

Table 2: Status of Outstanding Directives

Directive Summary	Issued Date	Order No./Para.	Docket	Project Number	Due Date	Status
S-Ref 10871: ¶ 6: "[W]e also direct NERC to develop a means to assure that IROLs are communicated to transmission owners." | ¶ 41: "NERC should establish a clearly defined communication structure to assure that IROLs and changes to IROL status are timely communicated to transmission owners." | ¶ 42: "We encourage NERC to inform us when it has developed means for communication of IROLs to transmission owners to help ensure that they receive notice of each of their applicable lines before the [FAC-003-2] standard becomes effective as to those lines. [that is, 'twelve months after the date a line operated below 200 kV is initially designated as an element of an IROL']"	3/21/13	Order No. 777 ¶ 6 ¶ 41 ¶ 42	RM12-4-000	2015-09 Establish and Communicate System Operating Limits	n/a	Ongoing.
S-Ref 10820: "[The Commission] believe[s] that NERC should register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System." | "NERC should consider whether there is a current need to register demand side aggregators and, if so, to address any related issues and develop criteria for their registration."	1/18/08	Order No. 706 ¶ 51	RM06-22-000	n/a	n/a	Ongoing.

Table 2: Status of Outstanding Directives						
S-Ref 10957: "[T]he Commission directs NERC, pursuant to Section 1600 of the NERC Rules of Procedure, to collect GIC monitoring and magnetometer data from registered entities for the period beginning May 2013, including both data existing as of the date of this order and new data going forward, and to make that information available."	9/22/16	Order No. 830 ¶ 89	RM15-11-000	n/a	n/a	Ongoing. Entities will be required to begin mandatory collection during designated GMD events beginning October 1, 2020. The first collection period will end on March 31, 2021. The first reporting deadline is June 30, 2021.
"[W]e… direct NERC to conduct a study to assess the implementation of Reliability Standard CIP-003-7. The study should address what electronic access controls entities choose to implement and under what circumstances, and whether the electronic access controls adopted by responsible entities provide adequate security, as well as other relevant information found by NERC as a result of the study. NERC must file the study within eighteen months of the effective date of Reliability Standard CIP-003-7."	4/19/18	Order No. 843 ¶ 30	RM17-11-000	n/a	7/1/21	On track to be filed by due date.
"We also find that it is reasonable for NERC to file annually an anonymized report providing an aggregated summary of the reported information, similar to the ICS-CERT annual report. The annual report will provide the Commission, NERC, and the public a better understanding of any Cyber Security Incidents that occurred during the prior year without releasing information on specific responsible entities or Cyber Security Events."	7/19/18	Order No. 848 ¶ 90	RM18-2-000	n/a	Annually, following the effective date of CIP-008-6.	Permanently ongoing. Initial report on track to be filed by due date.

Table 2: Status of Outstanding Directives						
"[W]e direct NERC to develop modifications to the CIP Reliability Standards to include EACMS within the scope of the supply chain risk management Reliability Standards. We direct NERC to submit the directed modifications within 24 months of the effective date of this final rule."	10/18/18	Order No. 850 ¶ 30	RM17-13-000	2019-03 Supply Chain Risks	12/26/20	On track to be filed by due date.
"[W]e direct NERC to prepare and submit a report addressing how often and why applicable entities are exceeding corrective action plan deadlines as well as the disposition of time extension requests. The report is due within 12 months from the date on which applicable entities must comply with the last requirement of Reliability Standard TPL-007-2."	11/15/18	Order No. 851 ¶ 30	RM18-8-000	n/a	1/1/25	On track to be filed by due date.
"[W]e direct that NERC develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers."	1/23/20	Order No. 866 ¶ 36	RM18-20-000	TBD	n/a	Standard Authorization Request accepted by NERC Standards Committee on 3/18/2020.
"NERC is directed to file quarterly status updates on Project 2016-02 and Project 2019-02, on an informational basis, starting 120 days from the date of issuance of this order."	2/20/20	Feb 20 Order 170 FERC ¶ 61,109 ¶ 1	RD20-2-000	2016-02 Modifications to CIP Standards 2019-02 BES Cyber System Information Access Management	Quarterly, beginning 6/19/20.	Ongoing. First update filed on 3/19/20.

Chapter 3: Conclusion

NERC is continuing to work closely with industry stakeholders and FERC to resolve all outstanding directives. Completing the majority of this work has provided the opportunity for industry to strategically review the standards and address as many directives as possible to date.

20200319-3015 FERC PDF (Unofficial) 03/19/2020

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

OFFICE OF ELECTRIC RELIABILITY

North American Electric Reliability Corporation
Docket No. RD20-3-000

March 19, 2020

North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, D.C. 20005

Attention: Lauren A. Perotti
Senior Counsel for North American Electric Reliability Corporation
Marisa Hecht
Counsel for North American Electric Reliability Corporation

Reference: Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard TPL-007-4

Dear Ms. Perotti:

On February 7, 2020, the North American Electric Reliability Corporation (NERC) filed a petition seeking approval of proposed Reliability Standard TPL-007-4 (Transmission System Planned Performance for Geomagnetic Disturbance Events).

NERC states that Reliability Standard TPL-007-4 requires owners and operators of the Bulk-Power System to conduct initial and on-going vulnerability assessments of the potential impact of defined geomagnetic disturbance events on Bulk- Power System equipment and the Bulk-Power System as a whole. NERC further states that the modifications in the proposed Reliability Standard address the Commission's directives in Order No. 851 related to requirements for corrective action plans.[1] Specifically, the Reliability Standard requires entities to develop corrective action plans for vulnerabilities identified through supplemental geomagnetic disturbance vulnerability assessments and requires entities to seek approval from the Electric Reliability Organization of any extensions of time for the completion of corrective action plan items.

[1] *Geomagnetic Disturbance Reliability Standard; Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*, Order No. 851, 165 FERC ¶ 61,124 (2018) at P 29 and P 54.

20200319-3015 FERC PDF (Unofficial) 03/19/2020

NERC's filed petition was noticed on February 11, 2020, with interventions, comments and protests due on or before March 9, 2020. No interventions or comments were received.

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 (2019), 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 (2019)

Sincerely,

Andrew Dodge, Director
Office of Electric Reliability

Document Content(s)

RD20-3-000.DOCX.....1-2

20200402-3034 FERC PDF (Unofficial) 04/02/2020

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. RR19-7-000

NOTICE OF EXTENSION OF TIME

(April 2, 2020)

On January 23, 2020, the Commission issued an order on North American Electric Reliability Corporation's (NERC) five-year performance assessment that directed NERC to make two compliance filings.[1] On March 19, 2020, the Secretary of the Commission issued a notice extending until May 1, 2020, deadlines for certain filings required by the Commission for those entities that are unable to meet deadlines due to steps they have taken to meet the emergency conditions related to the Novel Coronavirus Disease (COVID-19). NERC's compliance filing(s) providing certain information on its regional audits, guidance development program, Electricity Information Sharing and Analysis Center, and sanction guidelines is currently due on May 1, 2020. NERC's compliance filing(s) providing revisions to its Rules of Procedure is currently due on August 28, 2020. Due to the emergency conditions related to COVID-19, it is appropriate to extend these deadlines.

Upon consideration, notice is hereby given that NERC is granted an extension to comply with the Commission's directives in the January 23 Order. The compliance filing(s) providing information on its regional audits, guidance development program, Electricity Information Sharing and Analysis Center, and sanction guidelines is extended to and including June 1, 2020. The compliance filing(s) providing revisions to the NERC Rules of Procedure is extended to and including September 28, 2020.

Kimberly D. Bose,
Secretary.

[1] *North American Electric Reliability Corp.*, 170 FERC ¶ 61,029 (2020) (January 23 Order).

Document Content(s)

RR19-7-000 - Specl.DOCX.....1-1

20200417-3090 FERC PDF (Unofficial) 04/17/2020

171 FERC ¶ 61,052
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Neil Chatterjee, Chairman;
Richard Glick, Bernard L. McNamee,
and James P. Danly.

Disturbance Monitoring and Reporting Requirements Reliability Standard	Docket Nos. RM15-4-000
Coordination of Protection Systems for Performance During Faults and Specific Training for Personnel Reliability Standards	RM16-22-000
Supply Chain Risk Management Reliability Standards	RM17-13-000
North American Electric Reliability Corporation	RD18-4-000

ORDER GRANTING DEFERRED IMPLEMENTATION OF CERTAIN NERC RELIABILITY STANDARDS

(Issued April 17, 2020)

1. On April 6, 2020, the North American Electric Reliability Corporation (NERC) filed a motion seeking to defer the implementation of several Commission-approved Reliability Standards that have effective dates or phased-in implementation dates that fall in the second half of 2020. NERC requests a three-month deferral of the implementation of Reliability Standards CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)), CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments), and CIP-013-1 (Cyber Security – Supply Chain Risk Management); and a six-month deferral of the implementation of Reliability Standards PRC-002-2 (Disturbance Monitoring and Reporting Requirements), PRC-025-2 (Generator Relay Loadability), PRC-027-1 (Coordination of Protection Systems for Performance During Faults), and PER-006-1 (Specific Training for Personnel). In this order, we grant NERC's motion.

20200417-3090 FERC PDF (Unofficial) 04/17/2020

I. Background

A. Section 215 and Mandatory Reliability Standards

2. Section 215 of the Federal Power Act (FPA) requires the Commission to certify an Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[1] Once approved, the Reliability Standards are enforceable in the United States by the ERO, subject to Commission oversight, or by the Commission independently.

B. COVID-19

3. On March 13, 2020, the President issued a proclamation declaring a national emergency concerning COVID-19. On March 18, 2020, the Commission and NERC issued a joint statement announcing they would use regulatory discretion when considering the impact of the COVID-19 pandemic on registered entities' ability to comply with Reliability Standards. In recognition of the impacts of the COVID-19 pandemic, the Commission also extended filing deadlines in reliability proceedings pending before the Commission.[2]

II. NERC's Motion

4. NERC requests that the Commission delay the implementation of Commission-approved Reliability Standards that are scheduled to become effective, in whole or in part, in the second half of 2020.[3] NERC requests that the Commission delay the implementation of these Reliability Standards by three to six months, as follows:

> (a) For Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1, NERC seeks to extend the implementation of these standards by three months, from the currently scheduled July 1, 2020 effective date to October 1, 2020.

[1] 16 U.S.C. § 824o (2018).

[2] *See Notice Granting Extension of Time*, Docket No. AD20-11-000 (Mar. 19, 2020); *Notice of Extension of Time*, Docket No. RM19-20-000 (Apr. 2, 2020); *Notice of Extension of Time*, Docket No. RR19-7-000 (Apr. 2, 2020); *Notice of Extension of Time*, Docket No. RM20-8-000 (Apr. 2, 2020).

[3] NERC Motion at 4.

20200417-3090 FERC PDF (Unofficial) 04/17/2020

(b) For the Reliability Standard PRC-002-2 phased-in 50% compliance requirement, NERC seeks to extend the implementation date by six months from the currently scheduled July 1, 2020 compliance date to January 1, 2021.

(c) For the Reliability Standard PRC-025-2 phased-in implementation of Attachment 1: Relay Settings, Table 1 Options 5b, 14b, 15b, and 16b, NERC seeks to extend the implementation date by six months from the currently scheduled July 1, 2020 compliance date to January 1, 2021.

(d) For Reliability Standards PER-006-1 and PRC-027-1 and the associated new and revised NERC Glossary definitions, NERC seeks to extend the implementation of these standards by six months, from the currently scheduled October 1, 2020 effective date to April 1, 2021.

5. NERC states that it filed its motion to help ensure grid reliability amid the impacts posed by COVID-19.[4] NERC notes that the Commission and NERC have taken steps in recognition of the "critical importance of the reliability of the nation's energy sector and the steps that registered entities are taking to maintain the health and safety of their workforce and communities."[5] NERC asserts that delaying the implementation of these Reliability Standards is consistent with the actions taken by the Commission and NERC to address the impacts of COVID-19.[6]

6. NERC asserts that its motion is in the public interest and would not adversely impact reliability. NERC explains, in order to establish compliance with these Reliability Standards, registered entities would need to expend significant effort and resources in the coming months towards establishing and implementing processes and procedures, conducting the required coordination, and establishing documentation of compliance. NERC states that "[b]y providing for additional time and flexibility to establish compliance with new obligations, entities could continue to focus their immediate efforts and resources on maintaining the safety of their workforces and communities and ensuring the reliability of the grid during this public health emergency."[7]

[4] *Id.* at 2.

[5] *Id.* at 3.

[6] *Id.* at 4.

[7] *Id.* at 5.

20200417-3090 FERC PDF (Unofficial) 04/17/2020

III. Notice of Filing, Interventions and Answers

7. Notice of NERC's filing was issued on April 6, 2020 with answers or protests due on or before April 9, 2020. Reliable Energy Analytics LLC, the ISO/RTO Council, and the Joint Associations[8] filed timely answers in support of NERC's proposal, as described in NERC's filing. Commenters agree with NERC that the added flexibility provided by the delays would allow registered entities to recover from the impacts of the COVID-19 outbreak before implementing new controls and processes.[9]

8. Protect Our Power filed an out-of-time answer, suggesting that the Commission grant a shorter (i.e., 30-day) extension for Reliability Standard CIP-013-1 because of the critical nature of the utility industry supply chain and that many or most utilities may already be prepared to comply by the current July 1 deadline.[10] Michael Mabee (Mabee) filed an out-of-time protest, asserting that a pandemic was not unexpected and "the industry should have been prepared."[11]

IV. Procedural Matters

9. The unopposed motions to intervene are granted pursuant to the operation of Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2019).

10. Pursuant to Rule 213 of the Commission's Rules of Practice and Procedure, 18 C.F.R. §385.213 (2019), we reject the out-of-time answer and protest.[12]

---

[8] Edison Electric Institute, the American Public Power Association, the National Rural Electric Cooperative Association, and the Large Public Power Council.

[9] *See e.g.*, ISO/RTO Council Comments at 4; Joint Association Comments at 7.

[10] Protect Our Power Answer at 4.

[11] Mabee Protest at 2.

[12] Even if the answer and protest had been timely submitted, we would have denied them on the merits. We are unpersuaded that NERC's requested three-month extension "may not be in the public interest" and find that, although registered entities have taken steps to prepare for contingencies, it is nevertheless reasonable to provide them additional flexibility to properly allocate resources to address the impacts of COVID-19. NERC's requested extension allows entities to do so and NERC has indicated that granting the motion will not adversely impact the reliability of the Bulk-Power System.

20200417-3090 FERC PDF (Unofficial) 04/17/2020

V. Discussion

11. We grant NERC's motion and defer the implementation of Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 by three months, and the implementation of Reliability Standards PER-006-1, PRC-002-2, PRC-025-2, and PRC-027-1 by six months. We are persuaded by NERC's statement that granting this motion will allow registered entities to focus their immediate efforts and resources on maintaining safety and ensuring the reliability of the grid. Accordingly, we find that the deferred implementation dates constitute a reasonable and proportionate response to the substantial impacts of the COVID-19 pandemic on registered entities without unduly delaying the implementation of these Reliability Standards.

12. The Reliability Standards that are the subject of this order are important for ensuring the security and reliability of the grid. We recognize that registered entities have likely already taken significant steps to ensure the effective and timely implementation of these Reliability Standards, and we encourage them to continue doing so. Nevertheless, it is now necessary to balance the important role these NERC Reliability Standards play in protecting the reliability and security of the Bulk-Power System with the need for registered entities to respond to the immediate challenges of COVID-19. Therefore, we expect entities to continue their work in implementing the standards and to take advantage of the additional time to ensure they are fully compliant with these Reliability Standards when they become enforceable.

The Commission orders:

The Commission hereby grants NERC's motion to defer the implementation dates of certain Reliability Standards, as discussed in the body of this order.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

Document Content(s)

RM15-4-000.DOCX.....1-5

20200218-3034 FERC PDF (Unofficial) 02/18/2020

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF ELECTRIC RELIABILITY

North American Electric Reliability Corporation
Docket No. RD20-1-000

February 18, 2020

North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, D.C. 20005

Attention: Edward Schwerdt
President and CEO of Northeast Power Coordinating Council, Inc.
James McGrane
Senior Counsel for North American Electric Reliability Corporation

Reference: Petition of the North American Electric Reliability Corporation for Approval of Proposed Regional Reliability Standard PRC-006-NPCC-2

Dear Mr. McGrane:

On December 23, 2019, the North American Electric Reliability Corporation (NERC) and Northeast Power Coordinating Council, Inc. (NPCC) filed a joint petition seeking approval of proposed regional Reliability Standard PRC-006-NPCC-2 (NPCC Automatic Underfrequency Load Shedding).

NERC and NPCC state that regional Reliability Standard PRC-006-NPCC-2 establishes consistent and coordinated requirements for the design, implementation, and analysis of automatic underfrequency load shedding (UFLS) programs among all NPCC applicable entities. These requirements are more stringent and specific than the NERC continent-wide UFLS Reliability Standard, PRC-006-3, and were established such that the declining frequency is arrested and recovered in accordance with NPCC performance requirements. NPCC revised currently effective Regional Reliability Standard PRC-006-NPCC-1 to remove redundancies with the Reliability Standard PRC-006-3, clarify obligations for registered entities, improve communication of island boundaries to affected registered entities, and provide entities with the flexibility to calculate net load shed for UFLS in certain situations.

20200218-3034 FERC PDF (Unofficial) 02/18/2020

NERC's filed petition was noticed on December 30, 2019, with interventions, comments and protests due on or before January 29, 2020. An errata notice issued on January 6, 2020 corrected the comment due date to be January 22, 2020. No interventions or comments were received.

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 (2019), 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 (2019)

Sincerely,

Andrew Dodge, Director
Office of Electric Reliability

Document Content(s)

RD20-1-000.DOCX.....1-2

170 FERC ¶ 61,109
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. RD20-2-000

ORDER DIRECTING INFORMATIONAL FILINGS REGARDING
NERC STANDARD DRAFTING PROJECTS

(Issued February 20, 2020)

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission directs the North American Electric Reliability Corporation (NERC) to submit an informational filing describing the activity of two NERC critical infrastructure protection (CIP) standard drafting projects pertaining to virtualization and cloud computing services. Specifically, NERC should submit a schedule for Project 2016-02 (Modifications to CIP Standards) and Project 2019-02 (BES Cyber System Information Access Management) (collectively, NERC Projects). Each schedule should include the current status of the project, interim target dates, and the anticipated filing date for new or modified Reliability Standards. NERC is directed to submit the informational filing within 30 days of the date of issuance of this order. In addition, we direct NERC to file quarterly status updates, on an informational basis, until such time as new or modified Reliability Standards are filed with the Commission.

I. Background

A. Project 2016-02 – Modifications to CIP Standards

2. NERC initiated Project 2016-02 in 2016 to address a directive in Order No. 822 regarding the protection of transient electronic devices used at low impact BES Cyber Systems.[2] The standard authorization request for the project that defines the scope of the drafting project includes matters beyond the Order No. 822 directive, including revisions

[1] 16 U.S.C. § 824o (2018). *See also* 18 C.F.R. § 39.2(d) (2019) (the electric reliability organization shall provide the Commission information as necessary to implement section 215 of the FPA).

[2] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, at P 32, *order denying reh'g*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

to support the use of virtualization technologies by registered entities as compatible with the CIP Reliability Standards.[3]

B. Project 2019-02 – BES Cyber System Information Access Management

3. NERC initiated Project 2019-02 in 2019 in response to an industry standard authorization request. The standard authorization request identified a need to enhance bulk electric system reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for responsible entities to manage their BES Cyber System Information. Specifically, Project 2019-02 is intended to facilitate the use of third-party data storage and analysis systems, in part by clarifying the minimum protections expected when a responsible entity utilizes third-party data management solutions (e.g., cloud computing services).[4]

II. Discussion

4. The Commission recognizes that the NERC Projects are ongoing and that substantial progress has been made by the standard drafting teams. As discussed in the Notice of Inquiry issued by the Commission regarding virtualization and cloud computing services, we are also aware of industry's interest in ensuring that the Reliability Standards do not unnecessarily impede the adoption of new technologies that could contribute to a more efficiently planned and operated Bulk-Power System.[5]

5. Given the potential importance of virtualization and cloud computing services, pursuant to section 215 of the FPA, the Commission directs NERC to submit an informational filing to update the Commission on the progress of Project 2016-02 and Project 2019-02. In particular, NERC should submit a schedule for each NERC Project that includes the current status of the project, interim target dates, and the anticipated filing date for new or modified Reliability Standards. NERC should submit the informational filing within 30 days of the date of issuance of this order. In addition, the Commission directs NERC to file quarterly status updates, on an informational basis, starting 120 days from the date of issuance of this order, until such time new or modified Reliability Standards are filed with the Commission.

---

[3] *See* North American Electric Reliability Corp., *Reliability Standards Under Development*, *https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx*.

[4] *See id.*

[5] *Virtualization and Cloud Computing Services*, Notice of Inquiry, 170 FERC ¶ 61,110 (2020).

The Commission orders:

(A) NERC is directed to make an informational filing for Project 2016-02 and Project 2019-02 within 30 days of the date of issuance of this order, as discussed in the body of this order.

(B) NERC is directed to file quarterly status updates on Project 2016-02 and Project 2019-02, on an informational basis, starting 120 days from the date of issuance of this order, as discussed in the body of this order.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

170 FERC ¶ 61,110
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

[Docket No. RM20-8-000]

Virtualization and Cloud Computing Services

(February 20, 2020)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of inquiry.

SUMMARY: The Federal Energy Regulatory Commission (Commission) seeks comments regarding the potential benefits and risks associated with the use of virtualization and cloud computing services in association with bulk electric system operations, as well as whether barriers exist in the Commission-approved Critical Infrastructure Protection Reliability Standards that impede the voluntary adoption of virtualization or cloud computing services.

DATES: Initial Comments are due **[Insert Date 60 days after date of publication in the FEDERAL REGISTER]**, and Reply Comments are due **[Insert Date 90 days after date of publication in the FEDERAL REGISTER]**.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways:

- Electronic Filing through http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
- Mail/Hand Delivery: Those unable to file electronically may mail or hand-deliver

comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.

- *Instructions*: For detailed instructions on submitting comments, see the Comment Procedures Section of this document.

FOR FURTHER INFORMATION CONTACT:

Patricia Ephraim Eke (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8388
Patricia.Eke@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
Kevin.Ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

170 FERC ¶ 61,110
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Virtualization and Cloud Computing Services Docket No. RM20-8-000

NOTICE OF INQUIRY

(February 20, 2020)

1. In this Notice of Inquiry (NOI), the Commission seeks comments on the potential benefits and risks associated with the use of virtualization and cloud computing services in association with bulk electric system operations. In addition, the Commission seeks comment on whether barriers exist in the Critical Infrastructure Protection (CIP) Reliability Standards, which are developed by the North American Electric Reliability Corporation (NERC) and approved by the Commission, that impede the voluntary adoption of virtualization or cloud computing services.

2. This NOI is an outgrowth of discussions concerning the potential benefits and risks associated with the adoption of virtualization and cloud computing services for bulk electric system operations at the Commission's June 27, 2019 Reliability Technical Conference and the March 28, 2019 Commission/Department of Energy (DOE) Security Investments for Energy Infrastructure Technical Conference.[1]

[1] The records of the June 27, 2019 Reliability Technical Conference and March 28, 2019 Commission/DOE conference are available on the Commission's eLibrary document retrieval system in Docket Nos. AD19-13-000 and AD19-12-000, respectively.

3. The Commission intends to use the record developed in this proceeding to determine whether it would be appropriate, pursuant to section 215(d)(5) of the Federal Power Act, to direct that NERC develop modifications to the CIP Reliability Standards to facilitate the voluntary adoption of virtualization and cloud computing services by registered entities.[2]

I. Background

A. Virtualization

4. 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.[3] Virtualization is commonly used in business applications and is managed through centralized software, referred to as a hypervisor, that manages multiple virtual computer resources that can be used by different processes, customers, clients, and users. A virtual environment can be a single program and the operating system on which it executes; a combination of multiple programs and associated operating systems, networks, computing environments, storage devices, or other such digital environments.

5. Virtualization can be used on a stand-alone basis in a bulk electric system control center environment to reduce capital and operating costs, increase the efficiency of

[2] 16 U.S.C. 824o(d)(5).

[3] *See* National Institute of Standards and Technology, *Guide to Security for Full Virtualization Technologies*, Special Publication 800-125 (Jan. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf.

existing computing assets, and improve incident recovery, among other reasons. Virtualization offers the potential for cost savings in asset management, including minimizing the need for physical assets, which require building space and procuring and maintaining physical computer hardware. A virtualized system can also be more quickly recovered than physical systems in the event of a malfunction or compromise.

6. Virtualization is a necessary technical enabler if the functions of BES Cyber Systems are to be moved to a cloud computing environment since a customer choosing to migrate one or more on-premise systems to the cloud will need to virtualize those systems for use in the cloud.[4]

B. Cloud Computing

7. The National Institute of Standards and Technology (NIST) Information Technology Laboratory Computer Security Resource Center defines cloud computing as 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."[5]

---

[4] BES Cyber System is defined as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." Glossary of Terms Used in NERC Reliability Standards, http://www.nerc.com/files/glossary_of_terms.pdf. The acronym BES refers to the bulk electric system.

[5] NIST, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

8. The primary cloud service models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These three cloud service models provide different levels of flexibility and control to organizations choosing to use cloud computing services. Entities may use cloud computing services for the simple storage of data or, as discussed above, to host and operate virtual systems used for bulk electric system operations. As a general matter, cloud computing enables entities to focus resources on providing core services, such as transmission or generation of electric energy, while outsourcing the IT infrastructure required to support them.

9. Leveraging cloud computing services in technology and business processes provides entities the opportunity to realize benefits in their IT operations, including greater scalability, greater flexibility and lower capital investment. Cloud computing services provide computing power and storage at a lower cost than maintaining in-house IT infrastructure while providing the capability for almost instantaneous expansion of services. Other potential benefits from the adoption of cloud computing services include enhanced access to data and applications due to the inherent redundancy and multiple pathways used to access cloud computing services.

C. Commission Technical Conferences

10. On June 27, 2019, the Commission held its annual Reliability Technical Conference to discuss four fundamental topics, including the impact of cloud-based

services and virtualization on bulk electric system operations, planning and security.[6] The technical conference addressed, among other things**:** (1) evolution of cloud computing and virtualization of cloud computing and virtualization technologies; (2) outsourcing risk; (3) Reliability Standards modifications; (4) appropriate systems for a cloud environment; and (5) security and non-security related benefits.

11. In general, panelists at the Reliability Technical Conference acknowledged the emergence of virtualization and cloud computing services and indicated that the Commission should take some action to address the use of these technologies for bulk electric system data management. Midcontinent Independent System Operator (MISO) recommended that the Commission further engage industry and cloud service providers in one or more technical conferences to clarify issues and direct timely industry action to establish a way forward with changes to CIP Reliability Standards specifically to accommodate the use of cloud computing services.[7] MISO explained that the benefits of virtualization include enhanced system recovery. In particular, MISO noted that during the past year it was able to recover virtual assets quicker than traditional computing assets when testing backup and recovery processes. American Public Power Association and Large Public Power Council, moreover, stated that if done with care, cloud computing

[6] FERC, Notice Inviting Post-Technical Conference Comments, Docket No. AD19-13-000 (Jul. 23, 2019).

[7] *See* Reliability Technical Conference, Docket No. AD19-13-000, Tr. 118:6-12 (Rosenthal).

solutions can reduce risk, increase flexibility and improve the security posture of the bulk electric system.[8]

12. During the Commission/DOE Security Investments for Energy Infrastructure Technical Conference on March 28, 2019, Southwest Power Pool (SPP) urged more flexibility regarding the use of cloud computing. SPP stated that it evaluated a number of products that would enable it to do a better job of protecting system data. SPP asserted the view that the currently-effective CIP Reliability Standards do not allow cloud-based technologies despite the fact that the vast majority of new products from many of its vendors are cloud-based. As an example, SPP stated that it:

> believes that it cannot deploy the required CIP controls for certain system information were it to be stored on externally-hosted servers (i.e., "the cloud"). Yet, we are finding that more and more vendors have flagship products that require all or a portion of CIP system information to be stored off-premises. This was a driving factor in our recent replacement of our service management software and has also been a complicating factor in the evaluation of vulnerability scanning and vulnerability management solutions. Hence, SPP has given weight to solutions that are more expensive or do not provide as much value as some cloud alternatives. The standards should not be so prescriptive as to force SPP to avoid industry trends that have proven to be secure, but not necessarily compliant.[9]

[8] Tr. 114:12-14 (Jacobs).

[9] *See* Nick Brown, Prepared Statement for Commission/DOE Security Investments for Energy Infrastructure Technical Conference, Docket No. AD19-12-000, at 3 (filed Apr. 2, 2019)

13. The concerns reflected in the comments from the two recent technical conferences have prompted the issuance of this NOI to seek additional comments on the benefits and risks associated with the use of virtualization and cloud computing services in association with bulk electric system operations. Further, to the extent that there are barriers in the currently-effective CIP Reliability Standards to their use, the Commission seeks comment on whether it is appropriate for the Commission to direct action to facilitate the voluntary adoption of virtualization and cloud computing services.

II. Request for Comments

14. In this proceeding, the Commission seeks comments on the potential benefits and risks associated with the use of virtualization and cloud computing services, as well as whether barriers may exist in the CIP Reliability Standards that impede the adoption of virtualization or cloud computing. Specifically, the Commission seeks comments on four general topics as part of this inquiry: (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 standards framework.

15. In the following sections, we pose questions that commenters should address in their submissions. However, commenters need not address every topic or answer every question identified below.

A. Scope of Potential Use of Virtualization and Cloud Computing Services

16. As discussed above, virtualization and cloud computing services offer a wide variety of potential uses in the context of users, owners and operators of the bulk electric system. Some entities may choose to utilize the cloud simply for data storage. Other entities may rely on virtualization and cloud storage to operate systems that control one or more core functions. Potential uses may include one or more of the BES reliability operating services described in the Guidelines and Technical Basis section of Reliability Standard CIP-002-5.1a (Cyber Security — BES Cyber System Categorization).[10] Specifically, it is possible that either virtualization or cloud computing services could be leveraged for the following reliability operating services:

- 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

17. Using BES reliability operating services as a point of reference to distinguish among possible applications of virtualization and cloud computing services in bulk electric system operations:

> A1. Identify and discuss which BES reliability operating services referenced above could be implemented in a virtualized environment.

---

[10] *See* Reliability Standard CIP-002-5.1a (Cyber Security — BES Cyber System Categorization), Guidelines and Technical Basis at 17-18.

A2. Identify and discuss which BES reliability operating services referenced above could be implemented in a cloud computing environment.

A3. Identify and discuss any other BES reliability operating or support services that could be implemented in a virtualized environment.

A4. Identify and discuss any other BES reliability operating, data storage or support services that could be implemented in a cloud computing environment.

B. Potential Benefits and Risks Associated with Virtualization and Cloud Computing Services

18. The Commission seeks comment on the potential benefits and risks associated with virtualization and cloud computing services:

B1. What are the potential benefits associated with adopting virtualization for the BES reliability operating services identified in response to Questions A1 and A3?

B2. Are there risks associated with adopting virtualization for the BES reliability operating services identified in response to Questions A1 and A3? If risks exist, discuss whether these risks can be effectively mitigated by a responsibility entity.

B3. What are the potential benefits associated with adopting cloud computing services for the BES reliability operating services, data storage and support services identified in response to Questions A2 and A4?

B4. Are there risks associated with adopting cloud computing services for the BES reliability operating services data storage and support services identified in response to Questions A2 and A4? If risks exist, discuss whether these risks can be effectively mitigated by a responsible entity.

B5. What are the potential benefits of relying on third-party assessments to ensure the secure use of virtualization and cloud computing services for BES reliability operations and support services?

B6. Discuss any risks associated with relying on third party assessments to ensure the secure use of virtualization and cloud computing services for BES reliability operations and support services and potential solutions to mitigate those risks.

C. Potential Impediments to Adopting Virtualization and Cloud Computing Services

19. As discussed above, during the Commission's 2019 annual Reliability Technical Conference, several commenters alluded to the fact that cloud-based offerings continue to increase as vendors are moving more of their services to the cloud.[11] Commenters further asserted that there is uncertainty on how virtualization and cloud computing services can be leveraged within the existing CIP framework. Similarly, at the March 2019 Commission/DOE Security Investments for Energy Infrastructure Technical Conference, a panelist asserted that there is uncertainty among registered entities on whether the CIP Reliability Standards allow cloud-based technologies "despite the fact that the majority of new products from many vendors are cloud-based."[12]

20. In light of the concerns expressed at these technical conferences, the Commission seeks comment on potential challenges with how the implementation of virtualization and cloud computing technologies will fit into the framework of the CIP Reliability Standards, and possible solutions to those challenges:

> C1. Provide comment on the validity of the panelists' concern discussed above and discuss the extent to which the trend toward cloud-based services could affect reliable and secure bulk electric system operations.
>
> C2. Are there any technical challenges in implementing virtualization technology for the BES reliability operating services identified in response to

---

[11] *See* June 27, 2019 annual Reliability Technical Conference, Transcript pages 113 and 115-116.

[12] *See* March 28, 2019, Commission/DOE Security Investments for Energy Infrastructure Technical Conference, Transcript page 128.

Question A1 that result from the current CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

C3. Are there any challenges in implementing virtualization technology for the BES reliability operating services identified in response to Question A1 that result from compliance obligations associated with the CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

C4. Are there any technical challenges in implementing cloud computing technology for the BES reliability operating services identified in response to Question A2 that result from the current CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

C5. Are there any challenges in implementing cloud computing technology for the BES reliability operating services identified in response to Question A2 that result from compliance obligations associated with the CIP Reliability Standards? Discuss how the CIP Reliability Standards could be augmented to address these challenges.

D. Potential Use of New and Emerging Technologies in the current CIP Standards Framework

21. The Commission seeks comment on potential new and emerging technologies beyond virtualization and cloud computing that responsible entities may be interested in adopting for the BES reliability operating services and if the CIP Reliability Standards would allow these technologies to be adopted.

D1. In addition to virtualization and clouding computing, discuss whether the CIP Reliability Standards limit the ability to take full advantage of new and emerging technologies for BES reliability operating services. Explain the types of new technologies, the potential benefits and how the CIP Reliability Standards may limit their use.

III. Comment Procedures

22. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice, including any related matters or alternative

proposals that commenters may wish to discuss. Comments are due [**Insert SERT Date 60 days after date of publication in the FEDERAL REGISTER**], and Reply Comments are due [**Insert Date 90 days after date of publication in the FEDERAL REGISTER**]. Comments must refer to Docket No. RM20-8-000, and must include the commenter's name, the organization they represent, if applicable, and their address.

23. 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.

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

25. 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.

IV. Document Availability

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

contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. eastern time) at 888 First Street NE, Room 2A, Washington, DC 20426.

27. 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.

28. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or email at ferconlinesupport@ferc.gov, or the Public Reference

Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By direction of the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

SUNSHINE ACT MEETING NOTICE

April 9, 2020

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:	April 16, 2020 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/.

1066th - MEETING

OPEN MEETING

April 16, 2020

10:00 AM

Item No.	Docket No.	Company
		ADMINISTRATIVE
A-1	AD20-1-000	Agency Administrative Matters
A-2	AD20-2-000	Customer Matters, Reliability, Security and Market Operations
		ELECTRIC
E-1	RM19-5-001	Public Utility Transmission Rate Changes to Address Accumulated Deferred Income Taxes
E-2	OMITTED	
E-3	OMITTED	
E-4	EL16-49-001	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.
	EL18-178-001 ER18-1314-002 (Consolidated)	PJM Interconnection, L.L.C.
E-5	EL16-49-002	Calpine Corporation, Dynegy Inc., Eastern Generation, LLC, Homer City Generation, L.P., NRG Power Marketing LLC, GenOn Energy Management, LLC, Carroll CountyEnergy 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.
	EL18-178-002 (Consolidated)	PJM Interconnection, L.L.C.

E-6	EL18-169-000	CPV Power Holdings, L.P., Calpine Corporation and Eastern Generation, LLC v. PJM Interconnection, L.L.C.
E-7	EL19-59-000	Consumers Energy Company v. Midcontinent Independent System Operator, Inc. and Michigan Electric Transmission Company, LLC
E-8	EL19-38-000	City and County of San Francisco v. Pacific Gas and Electric Company
E-9	ER20-511-002	Wilderness Line Holdings, LLC
E-10	ER20-519-000 TS20-2-000	Wilderness Line Holdings, LLC
E-11	ER19-211-001	Entergy Arkansas, Inc.
E-12	EC19-18-001	Entergy Services, LLC, Entergy Arkansas, Inc., Entergy Louisiana, LLC, Entergy Mississippi, Inc., Entergy New Orleans, LLC, and Entergy Texas, Inc.
E-13	OMITTED	
E-14	EL17-62-000	Potomac Economics, Ltd. v. PJM Interconnection, L.L.C.
E-15	EL18-183-000	Radford's Run Wind Farm, LLC v. PJM Interconnection, L.L.C.
E-16	OMITTED	
E-17	ER15-2563-002 EL15-95-002	PJM Interconnection, L.L.C. Delaware Public Service Commission and Maryland Public Service Commission v. PJM Interconnection, L.L.C. and Certain Transmission Owners Designated under CTOA RS FERC No. 42
E-18	ER19-105-004	PJM Interconnection, L.L.C.
E-19	ER19-6-003	Delmarva Power & Light Company and PJM Interconnection, L.L.C.
E-20	ER20-922-000	New York Independent System Operator, Inc.
E-21	ER19-1927-002	Portland General Electric Company
E-22	ER09-1165-000	Duke Energy Progress, LLC
E-23	ER19-1900-002	Golden Spread Electric Cooperative, Inc.
E-24	ER19-470-003	ISO New England Inc.
E-25	ER19-1920-002	Tampa Electric Company

E-26	EL10-65-006	Louisiana Public Service Commission v. Entergy Corporation, Entergy Services Inc., Entergy Louisiana, LLC, Entergy Arkansas, Inc., Entergy Mississippi, Inc., Entergy New Orleans, Inc., Entergy Gulf States Louisiana, L.L.C., and Entergy Texas, Inc.
	ER14-2085-002 ER11-3658-002 ER12-1920-002 ER13-1595-002 (Consolidated)	Entergy Services, Inc.

HYDRO

H-1	P-2266-102	Nevada Irrigation District
H-2	P-943-131	Public Utility District No. 1 of Chelan County, Washington
H-3	P-14858-002	McMahan Hydroelectric, LLC

CERTIFICATES

C-1	CP19-477-000	Mountain Valley Pipeline, LLC
C-2	CP20-2-000	National Fuel Gas Supply Corporation
C-3	CP17-101-001	Transcontinental Gas Pipe Line Company, LLC
C-4	CP18-18-001	Transcontinental Gas Pipe Line Company, LLC
C-5	RP20-41-001	PennEast Pipeline Company, LLC
C-6	CP18-46-002	Adelphia Gateway, LLC
C-7	CP19-104-001 CP19-103-001	Texas Eastern Transmission, LP Columbia Gas Transmission, LLC
C-8	OMITTED	
C-9	CP14-57-000	Freeport LNG Development, L.P.

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.

APRIL 2020
Commission Meeting Summaries

These are summaries of orders voted by the Federal Energy Regulatory Commission at its April 16, 2020 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.

FERC denies rehearing

E-1, *Public Utility Transmission Rate Changes to Address Accumulated Deferred Income Taxes*, Docket No. RM19-5-001. The order addresses requests for rehearing and clarification of Order No. 864. The order reaffirms the Commission's determinations in Order No. 864 that public utilities with transmission formula rates must propose tariff revisions to implement certain excess or deficient accumulated deferred income taxes (ADIT)-related mechanisms in their transmission formula rates as a result of the Tax Cuts and Jobs Act of 2017 and that public utilities with transmission stated rates will address any excess or deficient ADIT resulting from the Tax Cuts and Jobs Act in their next rate cases.

FERC denies rehearing, grants clarification

E-4, *Calpine Corporation, et al. v. PJM Interconnection, LLC*, Docket No. EL16-49-001, *et al.* The order denies requests for rehearing and grants requests for clarification of the Commission's June 29, 2018 order finding PJM's then-existing tariff unjust and unreasonable because it failed to protect the integrity of competition in the capacity market against the price-distorting impact of resources receiving out-of-market support.

FERC denies in part and grants in part requests for rehearing and clarification

E-5, *Calpine Corporation, et al. v. PJM Interconnection, LLC*, Docket No. EL16-49-002, *et al.* The order denies in part and grants in part requests for rehearing and clarification of the Commission's December 19, 2019 order determining the just and reasonable replacement rate for PJM's minimum offer price rule. The order also directs PJM to submit a compliance filing within 45 days of the issuance of the order.

FERC dismisses complaint as moot

E-6, *CPV Power Holdings, L.P., et al. v. PJM Interconnection, LLC*, Docket No. EL18-169-000. The order dismisses as moot a complaint filed against PJM alleging that PJM's minimum offer price rule (MOPR) is unjust and unreasonable. The order finds that the determination sought by petitioners was made by the Commission in a related proceeding, Docket No. EL16-49-000, *et al.* (PJM Capacity Market Proceeding) in an order issued June 29, 2018. The complaint also seeks a replacement MOPR, a matter subsequently addressed and rendered moot by a Commission order issued in the PJM Capacity Market Proceeding on December 19, 2019.

FERC grants in part a complaint

E-7, *Consumers Energy Co. v. Midcontinent Independent System Operator, Inc. and Michigan Electric Transmission Company, LLC*, Docket No. EL19-59-000. The order grants in part Consumers Energy's complaint challenging the inclusion of the Morenci Interconnection Project in the 2018 MISO Transmission Expansion Plan (MTEP) and alleging that the Morenci Project is a local distribution facility. The order finds that the Morenci Project is local distribution in accordance with the application of the Commission's seven-factor test and determines that the Morenci Project should not have been included in the 2018 MTEP.

FERC denies a complaint

E-8, *City and County of San Francisco v. Pacific Gas & Electric Company*, Docket No. EL19-38-000. The order denies a complaint filed by the City and County of San Francisco against PG&E alleging that PG&E is unjustly and unreasonably implementing its wholesale distribution tariff and treating San Francisco in an unduly discriminatory manner with respect to San Francisco's requests to interconnect its loads to PG&E's system at secondary voltages rather than at primary voltages.

FERC accepts a proposed tariff

E-9, *Wilderness Line Holdings, LLC*, Docket No. ER20-511-002. The order accepts a proposed open access transmission tariff (OATT) in anticipation of a proposed transaction pursuant to which Wilderness Holdings intends to acquire from Sky River LLC, a majority ownership interest in a nine-mile, 230 kV radial transmission line located in Kern County, California.

FERC grants waivers

E-10, *Wilderness Line Holdings, LLC*, Docket Nos. ER20-519-000 and TS20-2-000. The order grants Wilderness Holdings requests for waivers of the Standards of Conduct and the requirements to establish and maintain an Open Access Same-Time Information, because it meets the Commission's definition of a small public utility and its annual electric sales do not exceed more than four million MWh. Wilderness Holdings explains that it will own, operate or control only the Wilderness Line, a radial transmission line that is used to transmit energy produced by individual generating facilities to the transmission grid.

FERC denies rehearing and grants clarification

E-11, *Entergy Arkansas, Inc.*, Docket No. ER19-211-001. The order denies rehearing and grants clarification of the Commission's September 30, 2019 order accepting a Joint Ownership and Operating Agreement, pursuant to which the Entergy Operating Companies will jointly own undivided interests in two Transmission Control Centers and pursuant to which Entergy Services, LLC will continue to provide Control Center operations and maintenance services to the Entergy Operating Companies.

FERC denies rehearing and grants clarification

E-12, *Entergy Services, LLC,* Docket No. EC19-18-001. The order denies rehearing and grants clarification of the Commission's September 30, 2019 order that had authorized the transfer of undivided ownership interests in two transmission control centers from Entergy Services, LLC to the Entergy Operating Companies.

FERC dismisses a complaint

E-14, *Potomac Economics, Ltd. v. PJM Interconnection,* , Docket No. EL17-62-000. The order dismisses Potomac's complaint against PJM that alleged that PJM's tariff was unjust and unreasonable because it required external generators seeking to provide capacity to load within PJM to obtain a pseudo-tie. The order finds that Potomac failed to meet its burden to demonstrate that PJM's pseudo-tie requirement is unjust and unreasonable.

FERC directs a further compliance filing

E-15, *Radford's Run Wind Farm, LLC v. PJM Interconnection, LLC*, Docket No. EL18-183-000. The order finds that the PJM tariff required PJM to use the information available to PJM at the time it completed the System Impact Study for Radford's interconnection request when it evaluated the Radford Upgrade for Incremental Capacity Transfer Rights (ICTR). The order directs PJM to make a compliance filing within 60 days of the date of the order detailing its determination on ICTRs for the Radford Upgrade.

FERC denies rehearing

E-17, *PJM Interconnection, LLC*, Docket No. ER15-2563-002. The order denies rehearing of the Commission's April 22, 2016 order that addressed amendments to Schedule 12-Appendix A of the PJM tariff that assigned cost responsibility for transmission enhancements and expansions for the Artificial Island Project.

FERC denies rehearing

E-18, *PJM Interconnection, LLC,* Docket No. ER19-105-004. The order denies rehearing of the Commission's May 28, 2018 order that accepted PJM's quadrennial revision of its Variable Resource Requirement curve used in the Reliability Pricing Model. The order affirms the Commission's determination to accept PJM's selection of the CT H-class turbine as the Reference Resource.

FERC grants an uncontested waiver

E-20, *New York Independent System Operator, Inc.*, Docket No. ER20-922-000. The order grants NYISO's uncontested request for a prospective waiver of certain language in the definition of "Public Power Entity" in section 2.16 of NYISO's Market Administration and Control Area Services Tariff. The requested waiver is for a period of nine months and will allow NYISO to continue to grant unsecured credit, in the amount of up to $1 million annually each, to government entities that do not meet the current definition of a Public Power Entity, consistent with NYISO's current practice.

FERC partially accepts a filing, directs a further compliance filing

E-21, *Portland General Electric Company*, Docket No. ER19-1927-002. The order finds Portland General's filing partially complies with the requirements of Order Nos. 845 and 845-A and the Commission's directives in the November 2019 order on compliance. The order directs Portland General to submit a further compliance filing within 120 days of the issuance date of the order.

FERC denies a challenge

E-22, *Duke Energy Progress, LLC*, Docket No. ER09-1165-000. The order denies the North Carolina Electric Membership Corporation's Formal Challenge of Duke Energy Progress' 2018 Annual Update to its Formula Rate.

FERC partially accepts a filing, directs a further compliance filing

E-23, *Golden Spread Electric Cooperative, Inc.*, Docket No. ER19-1900-002. The order finds that Golden Spread's filing partially complies with the requirements of Order Nos. 845 and 845-A and the Commission's directives in the November 2019 order on compliance. The order directs Golden Spread to submit a further compliance filing within 120 days of the date of issuance of the order.

FERC denies rehearing

E-24, *ISO-New England Inc.*, Docket No. ER19-470-003. The order denies rehearing of the Commission's November 22, 2019 order accepting ISO-NE's Order No. 841 compliance filing, subject to a further compliance filing.

FERC partially accepts a filing, directs a further compliance filing

E-25, *Tampa Electric Company*, Docket No. ER19-1920-002. The order finds that Tampa Electric's compliance filing partially complies with the requirements of Order Nos. 845 and 845-A and the Commission's order on Tampa Electric's May 21, 2019 compliance filing. The order accepts Tampa Electric's filing and directs Tampa Electric to submit a further compliance filing within 120 days of the date of the Commission order.

FERC grants rehearing in part, denies rehearing in part

E-26, *Louisiana Public Service Commission v. Entergy Corp., et al.*, Docket No. EL10-65-006, *et al.* The order grants rehearing in part of Opinion No. 560 on certain issues involving accumulated deferred income taxes. The order also denies rehearing on the interruptible load issue.

FERC rules state waived water quality certification authority

H-1, *Nevada Irrigation District,* Project No. 2266-102. The order finds 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 certification regarding the relicensing of Nevada Irrigation District's Yuba-Bear Project No. 2266, located on the

Middle and South Yuba rivers, Bear River, and Jackson and Canyon creeks in Nevada, Placer and Sierra counties, California.

FERC approves power sales contracts beyond license term

H-2, *Public Utility District No. 1 of Chelan County, Washington*, Project No. 943-131. The order grants a request from Chelan PUD, licensee for the Rock Island Hydroelectric Project No. 943, to approve an agreement that provides for the sale of power from the Rock Island Project to Avista Corporation beyond the term of Chelan PUD's existing license for the project, as required by section 22 of the Federal Power Act. The project is located on the Columbia River in Chelan and Douglas counties, Washington.

FERC denies rehearing and stay requests

H-3, *McMahan Hydroelectric, L.L.C.,* Project No. 14858-002. The order denies requests for rehearing by PK Ventures and North Carolina Department of Environmental Quality of the Commission's September 20, 2019 order granting an original license to McMahan Hydro for the Bynum Hydroelectric Project No. 14858, located on the Haw River in Bynum, Chatham County, North Carolina. The order also denies a stay request from PK Ventures.

FERC denies protest and authorizes construction

C-1, *Mountain Valley Pipeline, LLC,* Docket No. CP19-477-000. The order denies a protest to Mountain Valley's prior notice request to construct and operate a new metering and regulating station and related facilities in accordance with its Part 157 blanket certificate in Monroe County, West Virginia. While the order authorizes Mountain Valley to construct and operate the proposed facilities under the Part 157 blanket certificate, the authorization is stayed until Mountain Valley receives appropriate federal permits, and the Director of the Office of Energy Projects lifts the stop-work order and authorizes Mountain Valley to continue constructing along portions of the mainline.

FERC authorizes certificate amendments, partially vacates certain authorizations

C-2, *National Fuel Gas Supply Corporation,* Docket No. CP20-2-000. The order grants National Fuel's requests to amend and vacate authorizations associated with its existing Queen storage facilities and Line Q, and the Line QP Project located in Forest and Warren counties, Pennsylvania, granted by the Commission in Docket No. CP16-28-000 in an order issued September 6, 2017. Specifically, the order: (1) amends the authorization to abandon by sale the Queen Storage Field, including associated base gas, and the Queen Compressor Station to reflect a new purchaser; (2) vacates the authorization to abandon by sale a segment of Line Q that National Fuel is now retaining;

and (3) vacates, in part, the certificate authorization to construct the new Line QP that would have replaced Line Q.

FERC denies rehearing and stay requests

C-3, *Transcontinental Gas Pipe Line Company, LLC*, Docket No. CP17-101-001. The order denies requests for rehearing and stay of the Commission's order granting authorization under section 7 under the Natural Gas Act for Transco's Northeast Supply Enhancement Project.

FERC denies rehearing and stay requests

C-4, *Transcontinental Gas Pipe Line Company, LLC,* Docket No. CP18-18-001. The order denies requests for rehearing and stay of the Commission's order granting authorization under section 7 under the Natural Gas Act for Transco's Gateway Expansion Project.

FERC denies rehearing and stay requests

C-6, *Adelphia Gateway, LLC,* Docket No. CP18-46-002. The order denies requests for rehearing and stay of the Commission's order granting Adelphia Gateway authority to acquire, construct and operate a new interstate pipeline system in Delaware and Pennsylvania

FERC denies rehearing request

C-7, *Texas Eastern Transmission, LP,* Docket No. CP19-104-001 and *Columbia Gas Transmission, LLC,* Docket No. CP19-103-001. The order denies Washington Gas Light's request for rehearing of the Commission's order granting Texas Eastern's and Columbia's proposal to abandon their natural gas exchange service under Rate Schedules X-128 and X-130.

FERC terminates certain authorizations for a liquefied natural gas project

C-9, *Freeport LNG Development, L.P.,* Docket No. CP14-57-000. The order grants a request from Freeport to terminate its March 28, 2014 authorization under section 3 of the Natural Gas Act to integrate and operate a boil-off gas chiller at its liquefied natural gas terminal on Quintana Island, near Freeport, Texas to stabilize and augment system operations. In its December 18, 2019 pleading, Freeport explained the BOG chiller is no longer needed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Misoperation of 87N Transformer Ground Differential Relays Causing Loss of Load

Primary Interest Groups
Distribution Providers (DPs)
Generator Operators (GOPs)
Generator Owners (GOs)
Transmission Operators (TOPs)
Transmission Owners (TOs)

Problem Statement
Gaps in implementing a modification and subsequent commissioning processes led to the omission of neutral connections for three separate transformer neutral differential relays, ultimately causing three simultaneous misoperations and a subsequent loss of load.

Details
A significant load area was supplied by a 345 kV transmission substation arranged in a ring bus configuration (see Figure 1) with 10 bus sections tied to one another by 10 circuit breakers. Five 345 kV transmission lines and five 345 to 138 kV auto-transformers were connected in an alternating supply-load arrangement wherein the lines serve as the supply and the auto-transformers draw load from the transmission system. The auto-transformers, rated at 420 MVA each, supply multiple area distribution substations via 138 kV radial transmission feeders. The area substations contained 65 MVA transformers that step down the voltage onto a common 13 kV bus that supplies many distribution load feeders. One of the multiple area substations is depicted in Figure 1.

Only four 65 MVA transformers can be connected to the 13 kV bus at any time, or the fault duty would exceed the breaker interrupting capability. The fifth transformer therefore serves as a spare on hot standby, energized on the high side, but with its low side 13 kV breaker kept open.

The loss of load event was initiated by a routine single-line-to-ground fault on one of the 13 kV distribution feeders. The protective relays on the feeder detected the fault and were in the process of clearing it by tripping the 13 kV feeder breaker connected to the area substation. Just prior to the completion of this tripping action, neutral or ground differential relays (ANSI/IEEE device designation: 87N) simultaneously misoperated on three of the four in-service transformers at the area substation.

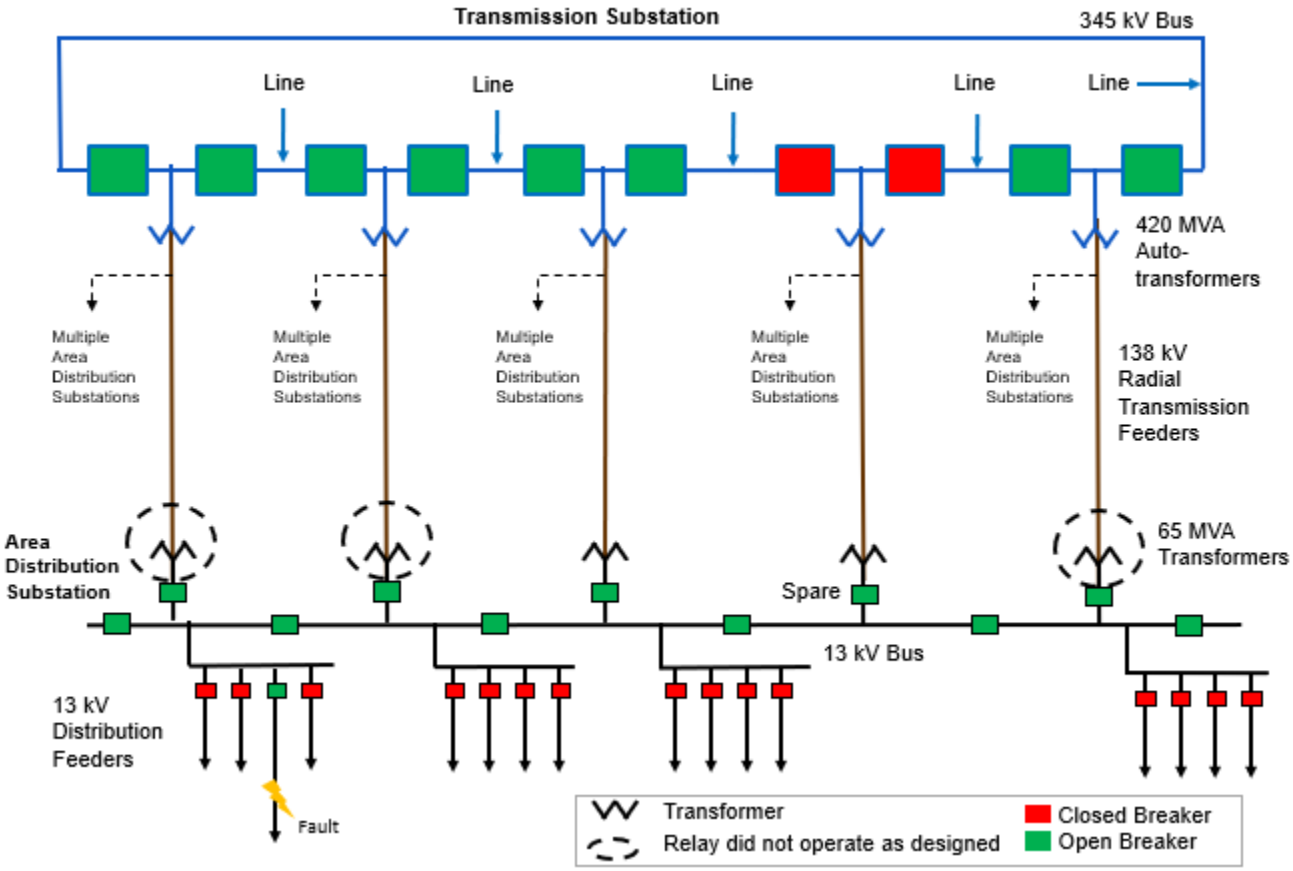


Figure 1: One-line Diagram of Transmission and Area Substations

The relays protecting the 65 MVA transformers at the area substations need to transfer trip the 345 kV ring bus breakers at the transmission substation in order to clear the source. Thus, the associated 420 MVA auto-transformer and 138 kV radial transmission feeder are tripped in tandem with the area substation transformer by design. The misoperations of 3 87N relays at the area substation therefore resulted in tripping 3 420 MVA autotransformers at the upstream transmission substation and the opening of 6 of the 10 ring bus breakers.

Immediately following the three 87N relay misoperations, the 13 kV distribution feeder breaker tripped to clear the fault in normal fashion. This was not a slow or stuck breaker scenario.

At this point, the entire load on the area substation bus was carried by the fourth and sole remaining in-service 65 MVA transformer. Within six seconds, prior to operators being able to switch in the hot standby spare transformer, the high-load current on the fourth transformer and resulting voltage drop across the transformer's impedance met the conditions to activate an automatic sectionalizing scheme on the 13 kV distribution bus. This segregated the area substation electrically into four segments, three of which already had lost their supply when the 87N relays misoperated, but this did not reduce the load current into the distribution network. The sectionalizing scheme then advanced to its next and final stage, tripping the

fourth transformer. That included opening two more breakers on the 345 kV ring bus at the transmission substation for a total of 8 out of 10.

The two 345 kV breakers that remained closed maintained the continuity of an important transmission path between two transmission feeders, permitting a portion of the load in the area to continue to be supplied to some of the area substations via the remaining autotransformer.

Event analysis and trouble-shooting determined that the three 87N relays on the area substation transformers misoperated due to an open or missing connection in the wiring between the 13 kV transformer secondary breaker current transformers (CTs) and the neutral auxiliary CT that supplies each 87N relay. This is depicted in schematic form in Figure 2. To function properly, the 87N relay requires inputs to compare the current through the transformer neutral itself to the ground current flowing through the secondary breaker as seen by the residual of the three phase currents. This missing connection unbalances the differential configuration.

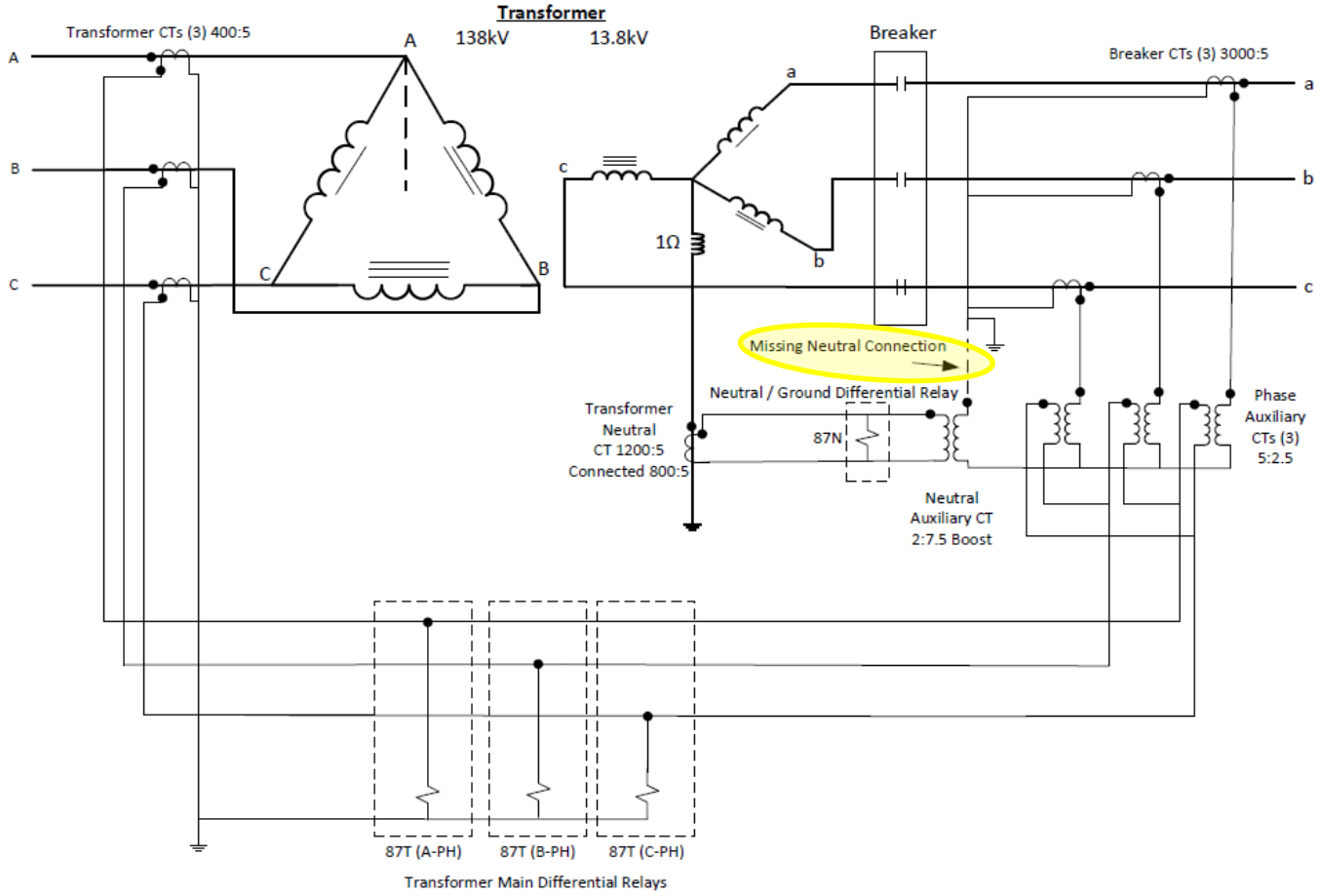


Figure 2: Schematic Diagram of Transformer Differential Relay Protection

Investigation found that the missing neutral connection occurred during a 13 kV breaker retrofit program undertaken many years after the substation was originally built. The vendor who performed the work opted to create a separate wiring diagram for the protective relay circuits that focused only on those portions of

the circuits being affected by the retrofit work. This separate diagram essentially took an excerpt of the overall transformer relaying circuit schematic and modified it to show connections to the upgraded breaker cabinet. It was intended to be used in conjunction with the original overall schematic, but it is believed that the wiring crew relied on it exclusively. This separate diagram lacked detailed terminal designations for the neutral-to-ground connection, thus one wire was landed on a termination where two were required.



Figure 3: Relay Panel Under Test Following the Event (87N In Lower Left Hand Corner)

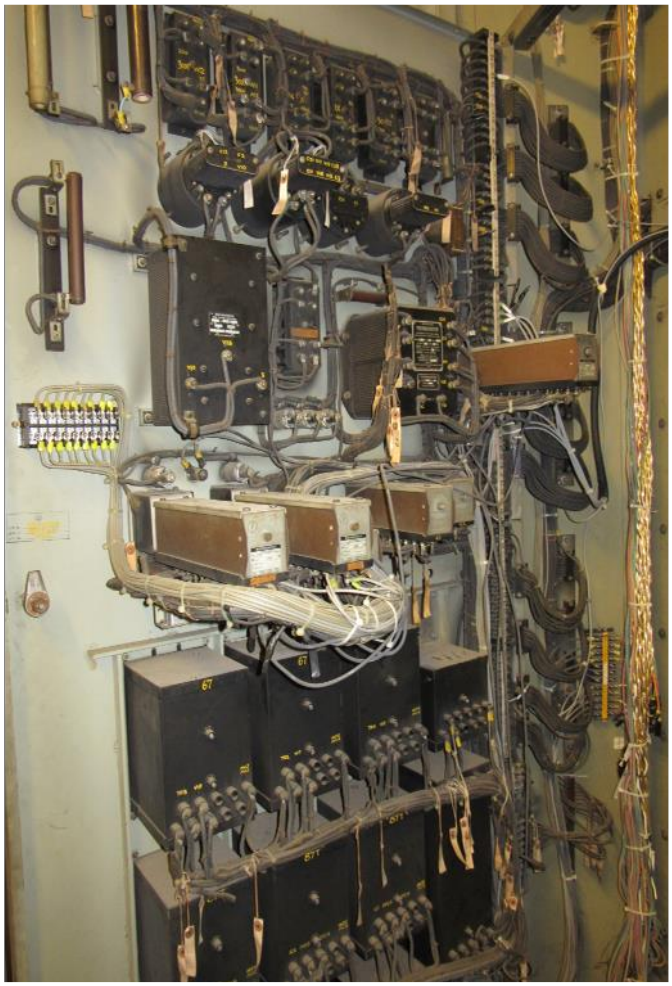


Figure 4: Wiring in Rear of Relay Panel

The error in connection existed on three transformers at the area substation for 10 years prior to the event. Although several 13 kV faults had occurred in the local distribution system over those 10 years, none had a sufficient combination of magnitude and duration to activate the 87N relays. The fourth transformer also had its 13 kV secondary breaker replaced, but that upgrade work was conducted several years later by a different crew. The same issue was present in its schematic drawings, was discovered during their review, and corrected. Consequently, the fourth transformer didn't trip during the event. Unfortunately, this new crew did not check to see if the same error existed on the earlier retrofits.

It is noteworthy that the problem was discovered during a drawing review on the last of the four transformers to have their breakers replaced but wasn't discovered during commissioning tests on the first

three. Primary current injection testing to validate the CT circuits was conducted when the breakers were replaced, but it focused on the circuits associated with the 13 kV bus and feeders. The transformer relaying was thought to be only peripherally affected by the upgrade, so this was not examined thoroughly. Separately but significantly, neutral or ground differential circuits present perhaps the greatest challenges for testing because polarities and connections cannot readily be validated with balanced phase currents. The presence of auxiliary CTs in the circuit complicates the matter even further.

Corrective Actions

The missing wiring was corrected (see Figure 5).



Figure 5: Added Neutral CT Connection to Complete 87N Circuit Post-Event

The first pair of process corrective actions were in the area of design and engineering. In order to reduce inconsistencies between drawings, a process was developed and implemented to redraw ac circuits with templates. This process change was aimed at reducing multiple drawings showing the same information for the same location. This avoids redundancy and the potential to introduce discrepancies between separate drawings. Furthermore, a set of human performance improvement checklists were expanded to support the review of critical circuits during the engineering phase of a project. The checklists adopt best practices from across the engineering departments.

Another area for improvement was in the standardization of commissioning testing for substation equipment and relay protection systems. The entity has two testing instructions in development to apply best practices from the industry and thereby prevent testing shortfalls. The two instructions include a guideline for commissioning and an instruction on primary injection testing methods. Both instructions are in draft form and are in the process of being vetted during actual construction projects now in progress.

Going forward, if a design discrepancy is found on a drawing or in the field, an “Extent of Condition” will be conducted. This involves assessing engineering drawing packages for similar projects to review and correct these discrepancies. This requirement will be captured in the design checklist during the engineering phase of a project. During the execution phase of a project, this requirement will be captured in the commissioning test instructions.

The underlying premise is that when a problem is encountered either in the design phase or the testing phase, the communication of the problem by way of feedback is essential to determining where else it may exist, thereby allowing it to be fully addressed to prevent reoccurrences elsewhere. The communication must be both within the organization that initially encountered the problem and between organizations that may be impacted either operationally or in terms of resources needed to mitigate the problem. The Extent of Condition approach is intended to weave this type of feedback into the fabric of conducting business, especially with respect to critical systems that have a direct bearing on safety and reliability of service.

When problems are uncovered that could potentially be encountered by other entities in the industry, these problems can and should be discussed in industry forums and, to the greatest possible extent, the pertinent information should be disseminated to the electricity sector. Discretion is needed to filter the problems that are worthy of communicating from those that aren't. In the case of this event, awareness of the root cause can clearly benefit the industry at large.

Lessons Learned

The event offers to the industry the four lessons listed below some of which have already been discussed in previous sections of the document.

- Improve Project Design Processes:
  - Apply thorough design review and comprehensive testing procedures be to the modification of any relay scheme.
- Standardize Commissioning Test Instructions:
  - Use standardized commissioning testing for substation equipment and relay protection systems.
  - Reference NERC and IEEE guidelines for developing and performing commission testing plans.[1]
  - The testing procedures should ensure that every piece of the relay scheme is tested in part and as a whole to determine deficiencies before they become latent weaknesses, particularly in cases of neutral relay schemes. Unlike phase differential relay schemes, in-service current measurements cannot be readily taken to determine a missing current transformer neutral connection.[2]
- Provide Feedback to Supervision and Engineering when Problems are Encountered:
  - Use Human Performance tools (such as STAR and Peer Checking) to check and recheck the wiring and connections of a relay circuit in its entirety. If there is conflicting information, do not proceed in the face of uncertainty – get knowledgeable help (i.e., ask supervision or engineering).

[1] IEEE PSRC, WG I-25 "Commissioning Testing of Protection Systems" https://www.pes-psrc.org/kb/published/reports/WG%20I-25%20Commissioning%20_Testing%20of%20Protection%20Systems%205-10-2017.pdf

[2] For additional insight into implementation and testing ground differential protection for transformers, see the paper "Considerations and Experiences in Implementing Ground Differential Protection for Transformer Protection at TVA" by Meyer Kao, Gary Kobet, and George Pitts. https://www.pes-psrc.org/kb/published/reports/TVA%20Ground%20Diffential%20Paper%20-%20GA%20Tech%20PRC%202009.pdf

  - Ensure accuracy and consistency of references provided for work – Avoid use of multiple drawings showing the same information for the same location to reduce the potential to introduce discrepancies that can occur between separate drawings.
  - When a design discrepancy is found on a drawing or in the field, it needs to be reported to engineering so an "Extent of Condition" can be conducted.
- Engineering should have a formalized process for conducting an "Extent of Condition" review to help ensure a consistent and thorough review is performed.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC is asking entities who have taken action on this lesson learned to respond to the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	NPCC – Event Analysis
Source of Lesson Learned:	Northeast Power Coordinating Council
Lesson Learned #:	20200401
Date Published:	April 14, 2020
Category:	Relaying and Protection Systems Transmission Facilities

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Protracted Fault in a Transmission Substation

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

Problem Statement
Electronic communications equipment utilized to transmit and receive information from the remote terminals of a transmission line automatically shut down within milliseconds when a bus fault occurred at one terminal of the line. Neither the primary nor the back-up relay protection cleared the fault. The fault continued for over four minutes.

Details
A single-phase-to-ground fault occurred on an instrument voltage transformer connected to the bus section that serves as the transmission line's terminal at Substation 1. The instrument voltage transformer was a capacitive coupling voltage transformer (CCVT)[1], comprised of a stack of coupling capacitors that form a voltage divider that supplies approximately 5 kV to a small potential device that in turn steps down the voltage to 120 volts for utilization by metering and back-up protective relaying. (See **Figure 1**). This instrument voltage transformer had exhibited low, out-of-tolerance output prior to the event. Low output voltage is often thought to be a benign condition for coupling capacitor devices.[2] The output to metering and back-up relaying had been temporarily isolated prior to the event to preclude false readings and avoid the risk of relay misoperation, but the coupling capacitors remained connected[3] to the transmission bus.

Communications equipment shut down at the substation where the fault occurred because of an electrical transient associated with the fault. The communication channels carried information utilized by the line differential relaying essential to the protection of the line and the bus sections at the line terminals.

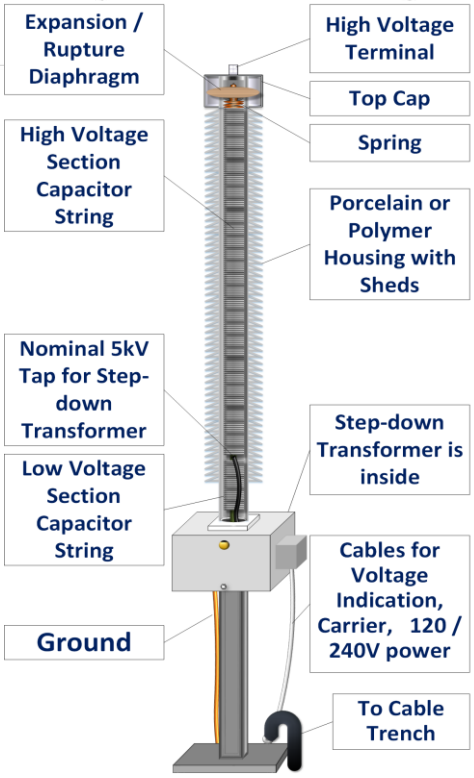


Figure 1: Typical CCVT

[1] CCVTs are one of the 14 common substation equipment types listed in the NERC Event Analysis' "Addendum for Events with Failed Station Equipment" for capturing failure modes and mechanisms in reported events.
[2] When capacitors begin to fail in a CCVT, it is usually by shorting out of individual capacitor packs in the string. If packs short out above the CCVT's "low voltage tap," the output voltage rises. If packs below the 'low voltage tap' short out, the output voltage would lower. In either case, there would be increased voltage stress across all the remaining capacitors in the string, accelerating their failure. As long as the string remains energized, this leads to a continuous sequence of shorting packs out and eventual catastrophic failure. Monitoring the output for "stair steps" can warn of a developing failure.
[3] The isolated output meant the condition of the capacitor string could not be monitored for the developing failure. It would have been better to remove power from the capacitors too. The difficulty of getting clearances for equipment that is expected to be "always on" contributed to leaving the equipment in this state for a long duration.

The transient, coupled to a 125-volt DC battery supply circuit in the substation by induction, activated a shutdown feature built into the electronic switching power supplies of the communications equipment. This feature was intended to protect the communications equipment against internal overloads on its printed circuit boards, chassis, and internal wiring. However, in this case, there was no internal overload. The shutdown feature misoperated in the presence of the transient because it carried an electrical or electronic signature similar to a bona fide overload condition within the communications equipment.

The instantaneous loss of communications prevented the line differential relaying from properly detecting the fault, so it blocked tripping by design. Stand-alone back-up relaying at the local substation where the fault occurred was temporarily out of service due to a problem with an instrument voltage transformer circuit. Stand-alone back-up relaying at one of the remote substations was slow in detecting the fault for several reasons, listed here:

- The line includes a series reactor with significant impedance (seven times more than the line impedance itself) for limiting fault current so as not to exceed interrupting capability of the circuit breakers. The impedance posed a challenge to setting the distance relay elements to ensure they did not over-reach to the next substation.
- The ratio of the impedance presented by the transmission line to a phase fault versus a ground fault is very different from the ratio presented by the series reactor. This results in the combined circuit (line and reactor) having an overall impedance that is non-homogeneous, posing another challenge to setting the distance relay elements.
- The fault evolved from a single-phase-to-ground fault to a three-phase-fault, then to a double-phase-to-ground fault, and finally back to a single-phase-to-ground fault. This evolution resulted in ground and phase distance elements alternately picking up and dropping out during the course of the event.

Figure 2 depicts the three-terminal transmission line involved in the event. One of the two redundant lines of primary line differential relaying is shown in a simplified format, including the communication equipment at two of the terminals. The third terminal is not included in the diagram for the sake of simplicity.

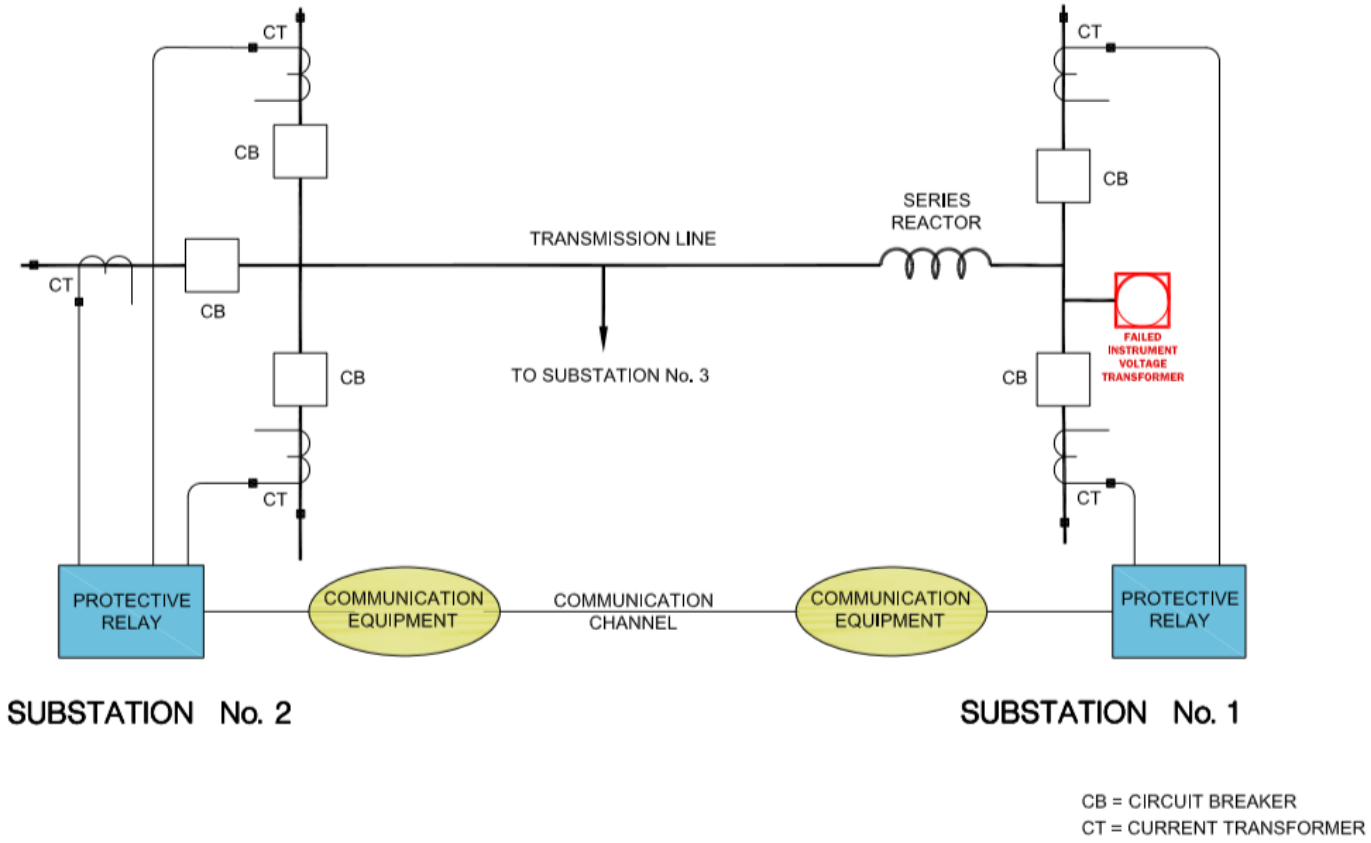


Figure 2: One Line Diagram of Faulted Circuit and Line Differential Protection

The fault was not cleared by either the primary or the back-up relay protection. It was determined from digital event files within the protective relays that communications between the relays for this circuit ceased simultaneously with the inception of the fault. Specifically, all four multiplexers associated with the line protection at Substation 1 had automatically shut down. The multiplexers are integral to the communications. They convert signals from the relays to a format suitable for transmitting over the digital telephone networks. **Figure 3** depicts the redundant double-triangular arrangement of the communication channels – Routes 1 and 2 – spanning all three terminals of the transmission line. It can be seen that each protective relay utilizes two multiplexers, one to connect to each of the two other substations.

The multiplexers were powered down even though their power switches were found in the ON position, and the 125 volt dc supplies from substation batteries were not interrupted. Each of the four multiplexers has two internal and independent electronic power supplies for the sake of redundancy. All eight internal electronic power supplies shut down automatically, which is the proximate cause of the loss of digital communications.

NOTE: If only one of the eight power supplies in the four multiplexers at Substation 1 had not shut down, the fault would have been cleared in normal high-speed fashion because the signals to and from Substation 1 would be exchanged with either Substation 2 or 3 as long as one route of communication remained between Substation 1 and either of the other two substations and then retransmitted between Substations 2 and 3, completing the triangular communications.

After the event, all eight of the power supplies were able to be restarted simply by manually cycling their power switches from ON to OFF and back to ON again. The multiplexers then resumed functioning, and normal communications were restored. There was no visible or functional damage to the multiplexers whatsoever. Neither the impacted electric utility nor the manufacturer is aware of this issue occurring prior to this event. The multiplexer equipment has a good track record of performance in the industry world-wide for many years.

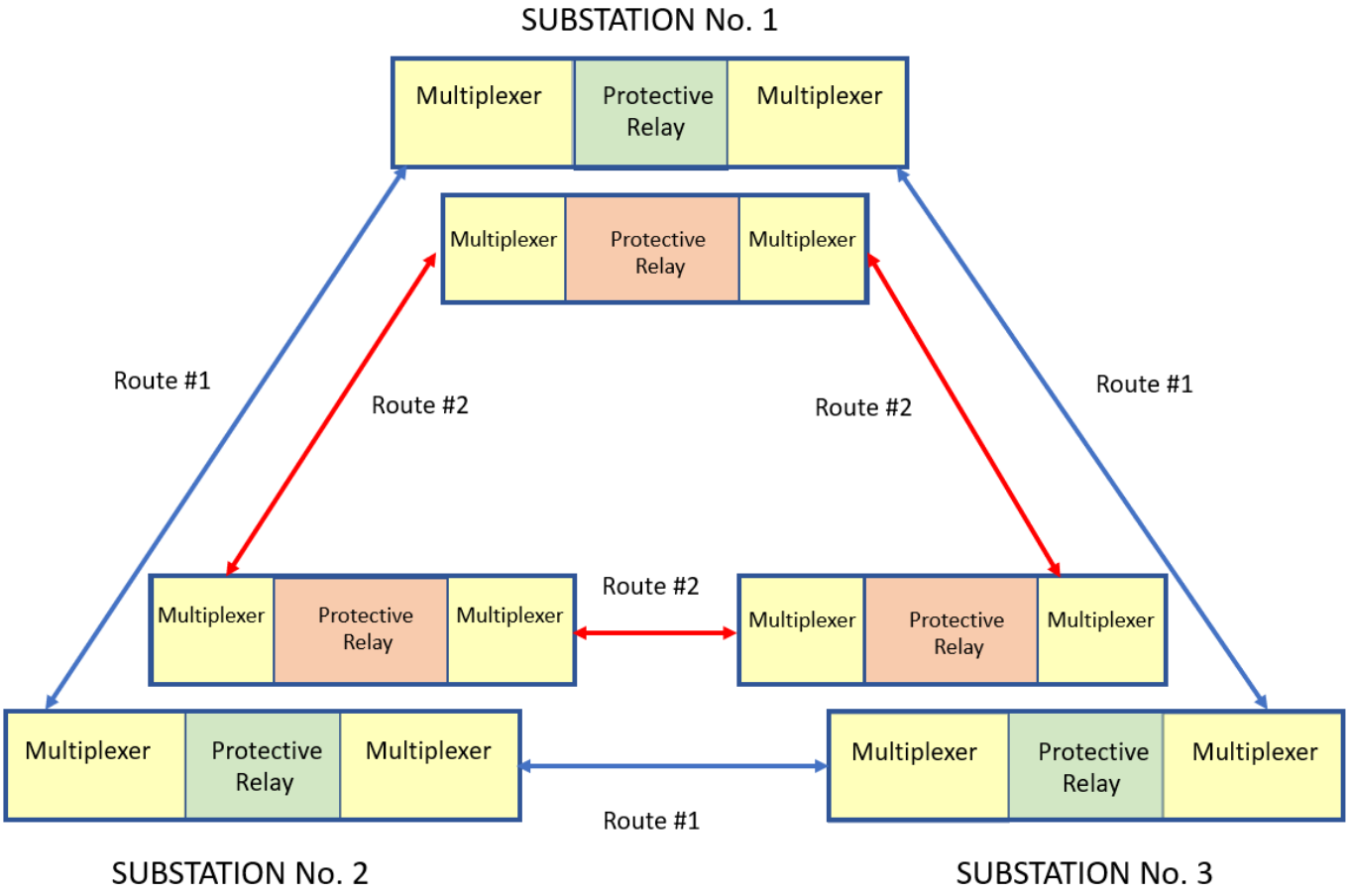


Figure 3: Redundant Communications for Three-Terminal Line

The shutdown was the result of activation of a control scheme on each power supply's printed circuit board that was intended to protect the power supply from overloading in the event of a short circuit within the multiplexer chassis or on any of its printed circuit boards, including those serving the communications functions. The scheme, when activated, inputs a signal into the integrated circuit chip that controls the switching cycle of the power electronics that simply stops the switching and holds it off until the power supply is manually restarted by toggling its ON-OFF rocker switch.

By design, the primary current differential relaying inhibited tripping when communications were lost. The loss of digital communication was simultaneous with the fault. Inhibiting tripping when communications are lost is necessary to prevent false tripping because the differential relays are unable to compare the

current flowing into the transmission line at one end to the current flowing out at the other end without communications.

As previously mentioned, an electrical transient generated by the fault on the Substation 1 bus section was coupled into the 125 volt dc battery supply circuit to the multiplexers. The exact mechanism of this coupling from an AC transmission fault into a dc supply circuit is not known. It was recognized, however, that the dc supply circuit was routed a considerable distance (~1000 feet) in substation trenches and cable trays shared with ac control wiring. It is typical the shielding is interrupted when cables enter and leave junction boxes. This offers a possible path for coupling by induction.

Another area that is typically of concern when problematic transients are generated by switching surges, lightning, or faults is substation grounding. Post-event testing revealed that the continuity between two adjacent ground grids in the affected area–one where the multiplexers reside and the other where the fault occurred–was less than desirable. This may have resulted in a more severe electrical transient being imposed on the multiplexer.

Post-event testing succeeded in recreating the shutdown scenario by selective switching on the power system. During this testing, a transient was captured that was subsequently reproduced by a signal generator and applied to the multiplexer power supplies, resulting in their shutdown. The electrical signature of this applied test transient waveform was different from those specified in the IEEE C37.90 standard for surge withstand capability. The standard includes both an oscillatory and fast transient test waveform. The test transient that resulted in the shutdown of the multiplexers was lower in amplitude and had a slower rate-of-rise than the IEEE waveforms but was of a longer duration. Thus, it fell outside the bounds of the standard. The multiplexer was designed to withstand the IEEE waveforms, and successfully passed when subjected to these waveforms.

Figures 4–7 show some of the damage that resulted from the event.



Figure 4: Failed C Phase CCPD



Figure 5: Damaged B Phase CCPD



Figure 6: Remnants of Bus Insulators



Figure 7: Exterior of Relay House Singed by Protracted Fault

Corrective Actions

All equipment damaged at Substation 1 during the fault was replaced. This included the instrument voltage transformer for the stand-alone back-up relaying that had been temporarily out of service.

The routing of the 125 volt DC supply feeds to the multiplexers that shut down during the event at Substation 1 has been significantly shortened, bypassing the long runs in control wiring trenches across the substation yard.

The ground grids at the affected substations have been reinforced.

An extent of condition review was conducted system-wide to identify locations where the type of multiplexer that shut down during the event is utilized for both the first and second line protective relaying. A fast-track effort was then embarked on to replace the power supplies in all of these multiplexers (two each) with power supplies that had been modified by the manufacturer to disable the shutdown scheme.

This was based on the underlying premise that it is preferable to sacrifice the power supplies within a multiplexer that develops an internal overload than to incorrectly shut down the unit and consequently disable a communications channel vital to the protective relaying. In addition, for all of the transmission lines associated with the substations involved in the event, the multiplexers on one of the two lines of

communication for every transmission line were replaced with new units of a different design and from a different manufacturer for the sake of diversifying the communications.

Going forward, all new and upgraded installations will utilize relays and communications equipment (multiplexers included) from different manufacturers for the first and second line protective relaying. This diversity of suppliers for redundant equipment is fundamental to the philosophy and design basis for protective relaying systems on transmission facilities.

Modifications of the stand-alone back-up relaying ensure coverage of the entire circuit with adequate margin so that the whole line, including any intermediary equipment, is sufficiently protected.

Lesson Learned

- Equipment that is out of service for maintenance, repairs, or replacement should be completely isolated. The maintenance, repair, or replacement work should then be conducted as quickly as possible to minimize potential compromises to system reliability.
- Control wiring routing and shielding should be designed to minimize the possibility of the coupling of transients between adjacent circuits.
- The functions served by protective relaying systems (including associated communications) are critical to the reliability of the transmission system. These functions, therefore, must have priority over schemes intended to monitor and react to problems internal to the individual components (e.g., electronics) that comprise the protective relaying systems. It's preferable to sacrifice an internal component than to have the protective system fail during a fault on the transmission system.
- Efforts should be made to have diversity in both the design and manufacture of all aspects of the protective relaying systems, including communications.
- Stand-alone back-up relaying must fully cover its intended protected zone with adequate margin for all types of faults.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC is asking entities who have taken action on this lesson learned to respond to the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	NPCC – Event Analysis
Source of Lesson Learned:	Northeast Power Coordinating Council
Lesson Learned #:	20200402
Date Published:	April 14, 2020

Category:	Relaying and Protection Systems Transmission Facilities

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Loss of Automatic Generation Control During Routine Update

Primary Interest Groups
Transmission Operators (TOPs)
Generation Operators (GOPs)
Balancing Authorities (BAs)
Reliability Coordinators (RCs)

Problem Statement
During a weekly automatic generation control (AGC) software update, a critical AGC task aborted at one of two fully redundant control centers, and the same critical task aborted at the other control center four minutes later. As a result, generation schedules could not be set, and area control error (ACE) could not be automatically calculated until the issue was resolved. The cause was a modified line of code.

Details
On December 10, 2019, a typical weekly AGC system build was being deployed. AGC was controlled from Control Center #1 with a completely redundant hot-standby system at Control Center #2. The standard process of work is to complete the deployment on the Control Center #2 AGC system and have the dispatcher transfer control to Control Center #2 AGC so the deployment can be completed on Control Center #1 AGC once that is complete. After the completion of that work, the dispatcher switches back to control using Control Center #1 AGC and remains in that state.

When the Control Center #2 AGC deployment was complete, the generation dispatcher was informed by software support staff that they could transfer control to the Control Center #2 AGC system so the software update could be completed on the Control Center #1 AGC system. Approximately 1 hour and 15 minutes after switching control to Control Center #2, a critical AGC task aborted and critical control functionality was lost. The software support staff immediately became aware of the problem and, after being unable to restart the task, advised the dispatcher to switch control back to Control Center #1 AGC since its software deployment had been completed. The dispatcher switched control to Control Center #1 AGC, and the same critical task aborted on the Control Center #1 AGC. At this point, the dispatcher contacted the generation plants under AGC control to confirm plant schedules and to instruct them to remain at their current generation levels. The RC was notified.

It was discovered that there was a change made to the primary inadvertent interchange (PII) alarm text during this AGC update that caused the failure. Prior to the update, when the PII value exceeded +/- 999 MW, the value in the alarm text defaulted to "****," preventing dispatchers from having an accurate indication of the amount of PII change. This alarm comes in when the PII value has a change greater than +/-200MW. During this deployment, the two MW value fields in the PII alarm text were modified from i4 to i5 (4 digit integers to 5 digit integers) to allow for an additional digit. While the dispatcher was controlling from the Control Center #2 AGC, the PII value went from +71 to +338 (267 MW change), causing the alarm. The original alarm text array had 79 characters which almost hit the max character limit of 80, and the

change from i4 to i5 resulted in the alarm text increasing by 2 characters to 81 characters in length. Writing an 81 character text string into an 80 character fixed length array resulted in a run-time abort of the task. When the dispatcher transferred control to the Control Center #1 AGC system, the Control Center #1 system began processing alarms and issued the same PII alarm, resulting in the same task to abort and loss of critical functionality on the Control Center #1 AGC. To immediately remedy the problem, code was written to tell the critical task to ignore the PII alarm. The dispatcher was able to go back on control on Control Center #1 AGC. Later that day, a more permanent remedy was implemented, and the alarm text statement was shortened to 72 characters while still allowing 5 digits in the MW value fields.

PRIOR TO BUILD: LARGE CHANGE IN PII FROM XXXX TO XXXX MW. SELECT ACCEPT TO ALLOW PII TO UPDATE. (79 characters)

AFTER BUILD: LARGE CHANGE IN PII FROM XXXXX TO XXXXX MW. SELECT ACCEPT TO ALLOW PII TO UPDATE. (81 characters)

CURRENT: LARGE CHANGE IN PII FROM XXXXX TO XXXXX MW. SELECT ACCEPT TO UPDATE PII. (72 characters)

Corrective Actions

A script was written to parse alarm format strings to see the theoretical limit for string max length to determine if any other alarms have text lengths that exceed the local array character limit.

The process was modified by the group that programs and tests AGC modifications. Prior to an update occurring, there will be fields in the system used to track control center work to prove that the code was tested. The coder name, tester name, and test evidence that proves the successful test are required.

Lesson Learned

- No matter how small the change is, validate changes in a test environment first. This requires using a thorough test script for the changes.
- A completed software testing process is critical to guarantee that products meet their requirements. In general, the process has four components:
  - **Test Scope:** to define test environment requirements and setup, features/functions that need to be tested, documentations to refer and produce as output, approval workflows, etc.
  - **Test Design:** to design test cases that are necessary to validate the system/functions/features being built, against its requirements. Typically, regression testing and incremental testing are necessary
  - **Test Execution:** to execute tests in many different ways
  - **Test Closure:** to consider the exit criteria for signaling completion of the test cycle and readiness for a release

- After implementing a code change at a control center, allow it to have enough time to determine that no adverse condition has been introduced prior putting that center in control (operate parallel) and prior to attempting to implement the change on the other control center.
- Buffer overflows must be avoided by maintaining a high degree of correctness in code that performs buffer management. It has also long been recommended to avoid standard library functions that are not bounds checked. Well-written and tested abstract data type libraries that centralize and automatically perform buffer management, including bounds checking, can reduce the occurrence and impact of buffer overflows.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC is asking entities who have taken action on this lesson learned to respond to the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	WECC Event Analysis
Source of Lesson Learned:	WECC
Lesson Learned #:	20200403
Date Published:	April 14, 2020
Category:	Communications

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Recommendation to Industry

Coronavirus Disease (COVID-19) Pandemic Contingency Planning

Initial Distribution: March 10, 2020

Coronavirus Disease (COVID-19) is a respiratory disease caused by the SARS-CoV-2 virus, which was first identified in Wuhan, China on December 8, 2019. The virus has since spread internationally to include confirmed cases in the United States, Canada, and other countries. The U.S. Centers for Disease Control and Prevention (CDC) and Public Health Agency of Canada (PHAC) both assess the current risk to the American and Canadian public as "low" as of March 4, 2020, although it is anticipated that the number and geographic dispersion of infected patients will increase in the coming weeks to months. To ensure reliability through the potential range of future developments, organizations should understand and consider the actions discussed in the Recommendation.

[Why am I receiving this? >>]
[About NERC Alerts >>]

Status:	**Acknowledgement Required by Midnight Eastern on March 12, 2020** **Reporting Required by Midnight Eastern on March 20, 2020**
	**PUBLIC:** No Restrictions More on handling >>
Instructions:	This Level 2 NERC Alert provides specific recommended actions that NERC registered entities should consider in response to a particular issue. Pursuant to Rule 810 of NERC's Rules of Procedure, NERC registered entities shall (1) acknowledge receipt of this advisory within the NERC Alert System, and (2) report to NERC on the status of their activities in relation to this recommendation (as provided below). For U.S. entities, NERC will aggregate the responses and provide an anonymized report to the Federal Energy Regulatory Commission. This Level 2 NERC Alert is not the same as a Reliability Standard nor does it create a mandatory obligation to take the recommended actions. Your organization will not be subject to penalties for failure to implement the recommendations. Issuance of this recommendation, however, does not alter the requirements of any approved Reliability Standard nor excuse the failure to follow the practices discussed in the recommendation if such failure constitutes a violation of a Reliability Standard. Registered entities must continue to comply with applicable Reliability Standards.

Distribution:	**Initial Distribution:** All Regions, All Entities, All Functional Groups Who else will get this alert? >>
Primary Interest Groups:	Cyber Security – Control Systems, Cyber Security – Corporate IT, Generation Engineering, Generation Operations, Generation Operations, Physical Security, System Operations – Transmission Engineering, System Operators, System Operators – System Protection, Transmission Planning
Recommendation:	This Recommendation to Industry, a Level 2 NERC Alert requests NERC registered entities to: • Acknowledge receipt of this advisory within the NERC Alert System. • Consider the recommendations below. • Review and complete the reporting instructions below. To the extent that Canadian jurisdictions have implemented laws or requirements that vary from Section 810 of the ROP, NERC requests that entities in such jurisdictions voluntarily participate in acknowledgement and reporting pursuant to this Alert. Recommendation #1: Develop and maintain suitable situational awareness of the current status of the spread of COVID-19 and credible future estimates of its spread and impacts. Incorporate the CDC's most current travel advisories into event planning and travel arrangements, and consider practices to increase awareness of employees' personal travel plans to areas with active advisories. Recommendation #2: Reinforce good personal hygiene practices across the workforce. Consider measures to increase the frequency and extent of cleaning and disinfecting surfaces and equipment that comes into routine contact with multiple people, particularly in business critical spaces or confined spaces that may be more conducive to disease communicability. Such areas may include control rooms, shared vehicles, conference rooms, and break areas. Consider implementing additional access restrictions such as limiting visitors or non-essential meetings within these spaces, and segregation of crews on shift work schedules. Recommendation #3: Review and update existing business continuity plans to ensure they are adequate to mitigate the direct impacts of a pandemic outbreak in the organization's footprint that creates staffing constraints for reliability and business functions. Recognize that a pandemic outbreak affecting the organization will also have similar effects on third-party contractors and supporting resources in the same footprint. Validate or develop thresholds and triggers for implementing increased flexible workforce

arrangements and for more disruptive mitigations, and ensure these mitigations are harmonious with guidance from the CDC or PHAC and local health agencies. Consider testing or exercising business continuity plans against a pandemic scenario.

Recommendation #4: Assess the organization's resilience against disruption to the availability of critical components, materials, and support resources with supply chains originating or traversing significantly impacted regions globally. At the present time, this includes China and nearby southeast Asian nations, so the most likely impact is expected to be to electronics, personal protective equipment and sanitation supplies, chemicals, and raw materials that are eventually transformed into goods directly purchased and used by North American asset owners and operators. Global transportation disruptions will also have ripple effects on the availability of these goods, particularly for "just-in-time" logistics systems. Organizations should work with their suppliers to understand current inventories of critical components throughout the supply chain as well as their anticipated use and resupply rates, and identify changed risks to routine, planned, and contingency operations to prioritize efforts appropriately.

Recommendation #5: Assess the need to adjust planned construction and maintenance activity schedules to prioritize the most important projects. Consider third-party support requirements and facility outage windows, and understand consumption rates of spare parts and supplies required for both planned and contingency work. Adjust plans as needed to maintain safe and reliable operations through potential workforce availability or supply chain disruptions.

Recommendation #6: Anticipate and prepare for coronavirus-themed opportunistic social engineering attacks. Spearphishing, watering hole, and other disinformation tactics are commonly used to exploit public interest in significant events. Take steps to ensure continued visibility and maintenance of cyber assets in the event of staffing disruptions. Ensure information and communications technology resources are appropriate to accommodate increased use of remote work arrangements consistent with business continuity plans, without compromising security. Consider conducting planned stress tests for these arrangements.

Reporting Instructions:

Initial acknowledgement of receipt is required by March 12, 2020, Midnight Eastern via the NERC Alert System. Responses to the questions below are required to be submitted via the NERC Alert System by March 20, 2020, Midnight Eastern.

A valid response in the NERC Alert System consists of the following three steps by the submitting entity:

1. Acknowledgement of Alert
2. Submission of Response
3. Approval of Response

The NERC Alert System contains menu options for each of the above commands that are available to authorized individuals upon login. A response will not be considered valid until all three steps have been completed.

All registered entities belonging to the Balancing Authority, Distribution Provider, Distribution Provider-UFLS, Frequency Response Sharing Group, Generator Owner, Generator Operator, Planning Authority, Reliability Coordinator, Resource Planner, Regulation Reserve Sharing Group, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, Transmission Service Provider functional groups are required to acknowledge receipt of this Alert and respond as applicable.

All registered entities covered by this Recommendation are required to provide an approved response as defined above to the following questions:

1. Does your organization have a written response plan, either standalone or incorporated into other written plans, which covers response to pandemic emergencies?

   A) Yes

   B) No, but we plan to develop one informed by this situation

   C) No, and we have no plans to develop one

2. Has your organization reviewed staffing requirements and resources for critical roles in a potential future COVID-19 pandemic emergency in North America?

   A) Yes

   B) No

3. In the event of a future COVID-19 pandemic emergency that does NOT directly impact your organization's geographic footprint, does your organization anticipate being able to offer traditional or non-traditional mutual aid to other industry participants, subject to appropriate agreements?

   A) Yes

   B) No

4. Has your organization reviewed supply chains for goods and services critical to reliable bulk power system operations that could be disrupted by the global COVID-19 pandemic emergency?

   A) Yes

   B) No

5. Does your organization presently anticipate any specific additional risks for the reliable and secure operations of your organization's portion of the bulk power system in a potential future COVID-19 pandemic emergency in North America?

   A) Yes

   B) No

6. If you answered A) Yes to Question 5, please briefly describe those specific risks your organization's portion of the bulk power system in the free-text entry box below.

   [1400-character entry box available in NERC Alert System]

Additional Information:

According to the CDC, COVID-19 can spread from person-to-person and is part of a larger family of viruses that are common in many different species of domesticated and wild animals. Other coronavirus variants that have affected the global community in the past include Severe Acute Respiratory Syndrome (SARS) in 2003, and the Middle East Respiratory Syndrome (MERS) in 2012.

Many of the details about this particular outbreak are still unclear, and epidemiological estimates continue to evolve with the spread of the virus. The following authoritative resources contain information about the virus, situational updates, and preventative measures:

- Coronavirus Disease 2019 (COVID-19) (CDC)
- Coronavirus Disease (COVID-19): Outbreak update (PHAC)

The Johns Hopkins Center for Systems Science and Engineering maintains a situational awareness tracker at Coronavirus COVID-19 Global Cases.

NERC's Electricity Sector Influenza Pandemic Planning, Preparation, and Response Reference Guide provides relevant industry-specific recommendations developed during the 2006-07 H5N1 Influenza pandemic.

The joint NERC and U.S. Department of Energy High-Impact, Low Frequency Event Risk to the North American Bulk Power System Summary Report (commonly referred to as the "HILF Report") contains guidance on pandemic

planning and preparation on pages 47-60; this guidance focuses on the staffing and direct business impacts.

The U.S. Department of Homeland Security's (DHS) 2006 Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources has additional advice and guidance.

Assessment processes for supply chain disruptions and resultant business risks from a pandemic is not fundamentally different from other geopolitical or socioeconomic causes. DHS's 2019 Supply Chain Resilience Guide gives an overview of these considerations.

The Electricity Subsector Coordinating Council (ESCC) maintains a consolidated list of online resources at the ESCC Workroom (login credentials required).

The E-ISAC has been monitoring this issue and sharing information with its members as it becomes available via the E-ISAC Portal, and will continue to do so. Continue to share voluntary information on situation assessments and unmet needs with E-ISAC and other trusted partners.

Contact:	Bulk Power System Awareness Group North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600 – North Tower Atlanta, GA 30326 404-446-9797 | nerc.alert@nerc.net
Alert ID:	R-2020-03-10-01

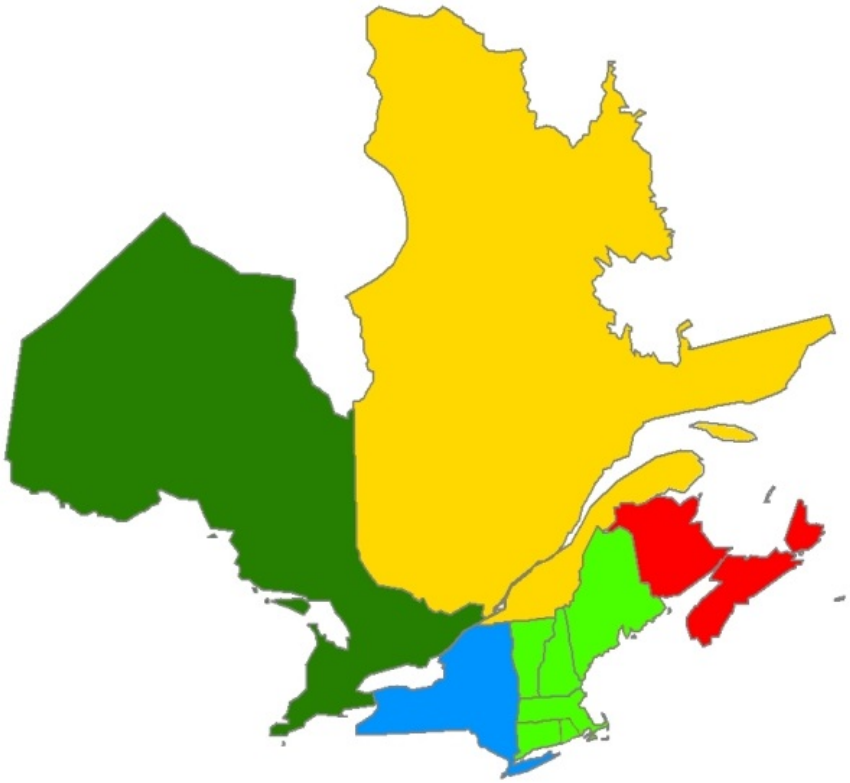
You have received this message because you are listed as a Primary Compliance Contact for your organization on the North American Electric Reliability Corporation's compliance registry, or an additional recipient designated by your Primary Compliance Contact. If you believe that you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact NERC via email at nerc.alert@nerc.net.

North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600 – North Tower
Atlanta, GA. 30326
404-446-2560
www.nerc.com

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**	$XXX,XXX	$XXX,XXX	
Regional Entity Division Assessments Percentage	**100%**	XX.X%	XX.X%	
Criteria Services Division Membership Fees	**$706,472**	$XXX,XXX	$XXX,XXX	
Total NPCC Assessments & Membership Fees	**$16,163,342**	$XXX,XXX	$XXX,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 (HQCMÉ), 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. HQCMÉ 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 NBUEB 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 EPAct 2005 to address the other functions listed above. These experts in operations, planning and reliability analysis assist registered entities in assessing and improving reliability. It is in support of these areas that NPCC engages the majority of industry experts on its technical committees.

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.

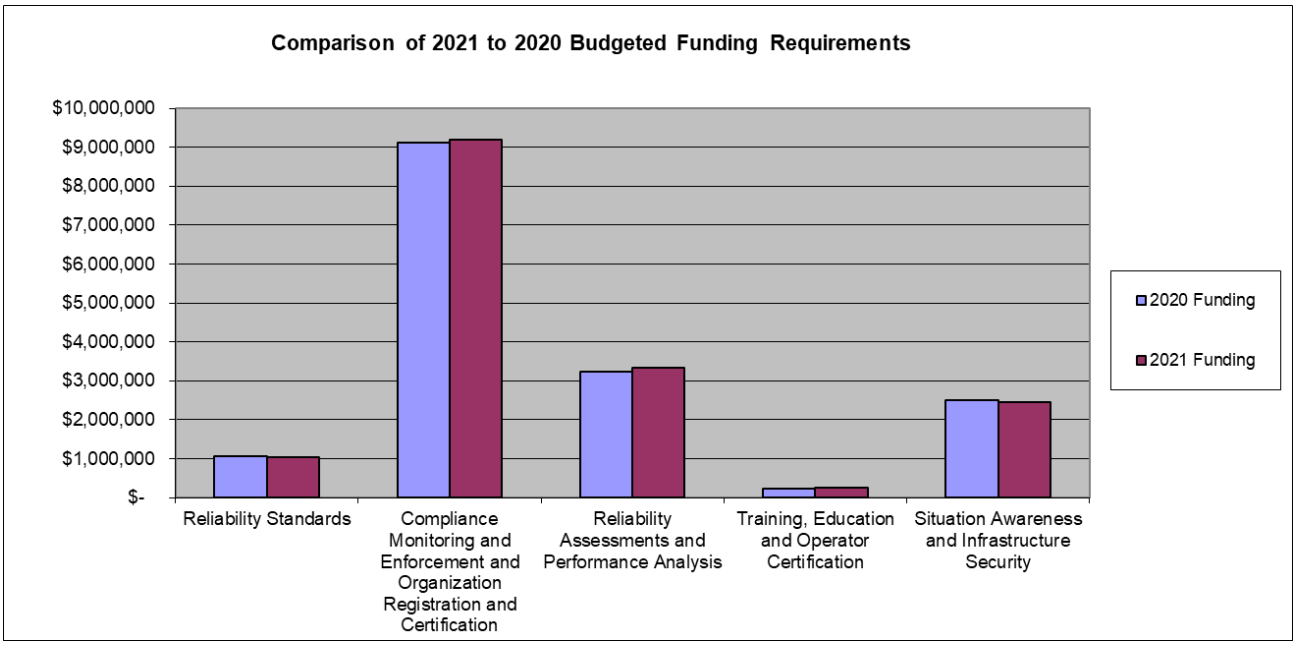
2020 Projections

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**

[1]A 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

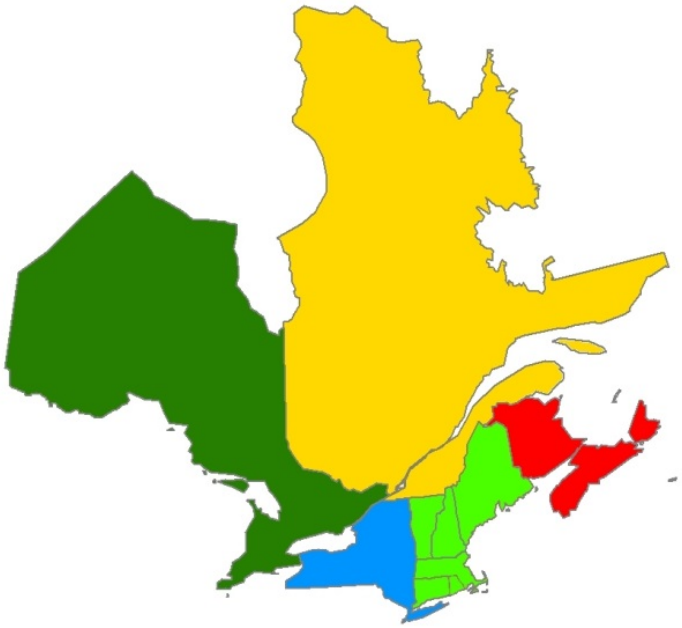
	2020 Budget	2020 Projection	Variance[2] 2020 Projection v 2020 Budget Over(Under)	2021 Budget[3]	Variance 2021 Budget v 2020 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 15,338,737	$ 15,338,737	$ -	$ 15,456,870	$ 118,133
Penalty Sanctions[1]	120,000	120,000	-	604,000	484,000
Total 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

	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	$ 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

  - Developing resilience metrics to better quantify the reliability enhancements of pre-event operations in a more secure state, reductions in the system degradation profile, and increasing the speed of recovery
  - 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
  - Developing Regional concurrence on appropriate levels of cyber resilience, the adequacy of security controls, and methodologies to simulate cyber impacts on BPS reliability
  - Expanding Regional support for and interaction with the E-ISAC and enhancing actionable information sharing within Northeastern North America
  - 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:
  - 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,
  - 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,
  - 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:
  - Supply Chain – new version of the Standard, more guidelines by RSTC's Supply Chain WG and industry (like NATF)
  - Virtualization – updates to several CIP Standards
  - IEC 61850 – addressing a gap in cyber security because it is excluded from CIP
  - CIP-012 implementation
  - CIP-008 – new version which requires notifying E-ISAC and United States National Cybersecurity and Communications Integration Center (NCCIC)
  - IST-4 WG – patch management of relays
  - Grid Ex VI (2021)
  - 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.

  - Assisting in the development and performance of real-time operating tools ensuring cyber security concerns are addressed.
  - 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:
  - 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.
  - Promote NPCC's Event Analysis group's process for sharing and dissemination of the detailed Event Analysis Report information among industry participants (registered entities).
  - 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).
  - 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.
  - 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 2021Business 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.

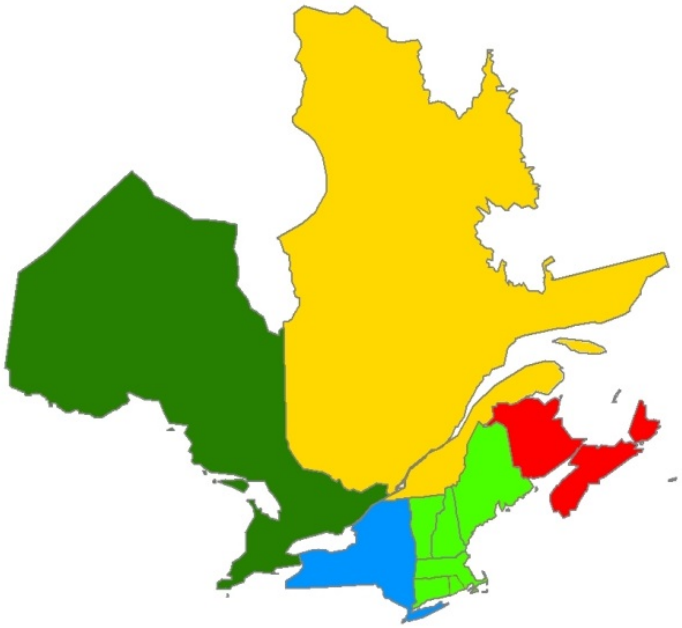
Any penalty monies received from NPCC registered entities within the U.S. by June 30th of the year preceding the business plan and budget year are then allocated among the NPCC program areas based on their FTE ratio and between the U.S. BAAs based on their relative NELs, and then added to the total compliance 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

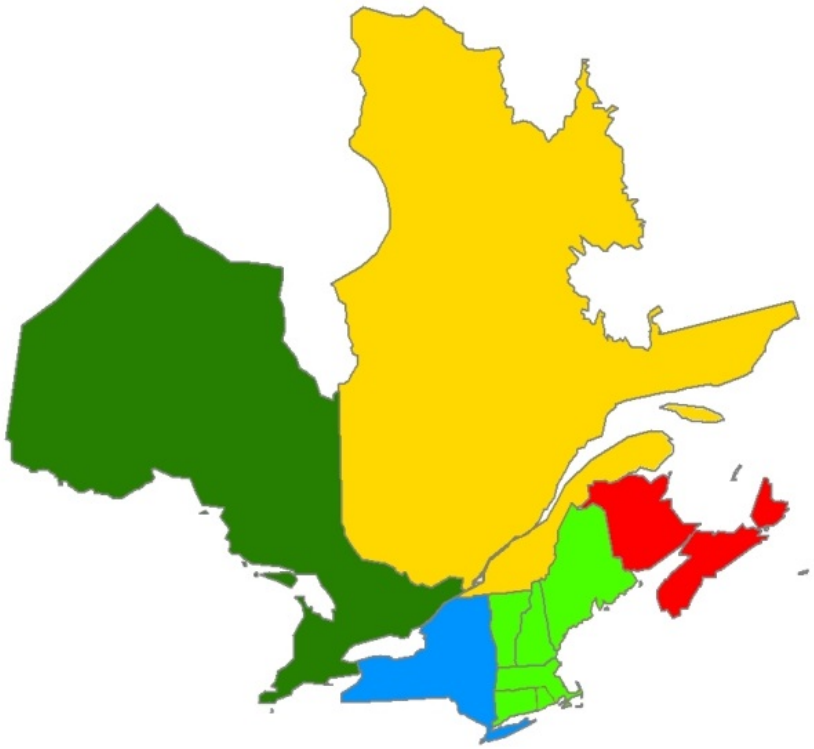
- Computer and software capital expenditures include the implementation of a security controls framework and data loss prevention strategy, as well as continuing enhancement of the document management system and equipment upgrades.
- Other planned capital expenditures include reconfigurations of office space related to succession planning.

Table B-13

To be Inserted

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 Understating 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 FTEs1 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**

[1]A 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.

EXECUTIVE ORDER

- - - - - - -

SECURING THE UNITED STATES BULK-POWER SYSTEM

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq*.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq*.) (NEA), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign adversaries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system, which provides the electricity that supports our national defense, vital emergency services, critical infrastructure, economy, and way of life. The bulk-power system is a target of those seeking to commit malicious acts against the United States and its people, including malicious cyber activities, because a successful attack on our bulk-power system would present significant risks to our economy, human health and safety, and would render the United States less capable of acting in defense of itself and its allies. I further find that the unrestricted acquisition or use in the United States of bulk-power system electric equipment designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in bulk-power system electric equipment, with potentially catastrophic effects. I therefore determine that the unrestricted foreign supply of bulk-power system electric equipment constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of

the United States, which has its source in whole or in substantial part outside the United States. This threat exists both in the case of individual acquisitions and when acquisitions are considered as a class. Although maintaining an open investment climate in bulk-power system electric equipment, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced with the need to protect our Nation against a critical national security threat. To address this threat, additional steps are required to protect the security, integrity, and reliability of bulk-power system electric equipment used in the United States. In light of these findings, I hereby declare a national emergency with respect to the threat to the United States bulk-power system.

Accordingly, I hereby order:

Section 1. Prohibitions and Implementation. (a) The following actions are prohibited: any acquisition, importation, transfer, or installation of any bulk-power system electric equipment (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the equipment), where the transaction was initiated after the date of this order, and where the Secretary of Energy (Secretary), in coordination with the Director of the Office of Management and Budget and in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other executive departments and agencies (agencies), has determined that:

(i) the transaction involves bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(b) The Secretary, in consultation with the heads of other agencies as appropriate, may at the Secretary's discretion design or negotiate measures to mitigate concerns identified under section 1(a) of this order. Such measures may serve as a precondition to the approval by the Secretary of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.

(d) The Secretary, in consultation with the heads of other agencies as appropriate, may establish and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system electric equipment market as pre-qualified for future transactions; and may apply these criteria to establish and publish a list of pre-qualified equipment and vendors. Nothing in this provision limits the Secretary's authority under this section to prohibit or otherwise regulate any transaction involving pre-qualified equipment or vendors.

Sec. 2. Authorities. (a) The Secretary is hereby authorized to take such actions, including directing the timing and manner of the cessation of pending and future transactions prohibited pursuant to section 1 of this order, adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA as may be necessary to implement this order. The heads of all agencies, including the Board of Directors of the Tennessee Valley Authority, shall take all appropriate measures within their authority as appropriate and consistent with applicable law, to implement this order.

(b) Rules and regulations issued pursuant to this order may, among other things, determine that particular countries or persons are foreign adversaries exclusively for the purposes of this order; identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries exclusively for the purposes of this order; identify particular equipment or countries with respect to which transactions involving bulk-power system electric equipment warrant particular scrutiny under the provisions of this order; establish procedures to license transactions otherwise prohibited pursuant to this order; and identify a mechanism and relevant factors for the negotiation of agreements to mitigate

concerns raised in connection with subsection 1(a) of this order. Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order.

(c) The Secretary may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary pursuant to this section within the Department of Energy.

(d) As soon as practicable, the Secretary, in consultation with the Secretary of Defense, the Secretary of the Interior, the Secretary of Homeland Security, the Director of National Intelligence, the Board of Directors of the Tennessee Valley Authority, and the heads of such other agencies as the Secretary considers appropriate, shall:

(i) identify bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States, poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States, or otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(ii) develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system.

Sec. 3. Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security. (a) There is hereby established a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security (Task Force), which shall work to protect the Nation from national security threats through the coordination of Federal Government procurement of energy infrastructure and the sharing of risk information and risk management practices to inform such procurement. The Task Force shall be chaired by the Secretary or the Secretary's designee.

(b) In addition to the Chair of the Task Force (Chair), the Task Force membership shall include the following heads of agencies, or their designees:

(i) the Secretary of Defense;

(ii) the Secretary of the Interior;

(iii) the Secretary of Commerce;

(iv) the Secretary of Homeland Security;

(v) the Director of National Intelligence;

(vi) the Director of the Office of Management and Budget; and

(vii) the head of any other agency that the Chair may designate in consultation with the Secretary of Defense and the Secretary of the Interior.

(c) The Task Force shall:

(i) develop a recommended consistent set of energy infrastructure procurement policies and procedures for agencies, to the extent consistent with law, to ensure

that national security considerations are fully integrated across the Federal Government, and submit such recommendations to the Federal Acquisition Regulatory Council (FAR Council);

(ii) evaluate the methods and criteria used to incorporate national security considerations into energy security and cybersecurity policymaking;

(iii) consult with the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council in developing the recommendations and evaluation described in subsections (c)(i) through (ii) of this section; and

(iv) conduct any other studies, develop any other recommendations, and submit any such studies and recommendations to the President, as appropriate and as directed by the Secretary.

(d) The Department of Energy shall provide administrative support and funding for the Task Force, to the extent consistent with applicable law.

(e) The Task Force shall meet as required by the Chair and, unless extended by the Chair, shall terminate once it has accomplished the objectives set forth in subsection (c) of this section, as determined by the Chair, and completed the reports described in subsection (f) of this section.

(f) The Task Force shall submit to the President, through the Chair and the Director of the Office of Management and Budget:

(i) a report within 1 year from the date of this order;

(ii) a subsequent report at least once annually thereafter while the Task Force remains in existence; and

(iii) such other reports as appropriate and as directed by the Chair.

(g) In the reports submitted under subsection (f) of this section, the Task Force shall summarize its progress, findings, and recommendations described in subsection (c) of this section.

(h) Because attacks on the bulk-power system can originate through the distribution system, the Task Force shall engage with distribution system industry groups, to the extent consistent with law and national security. Within 180 days of receiving the recommendations pursuant to subsection (c)(i) of this section, the FAR Council shall consider proposing for notice and public comment an amendment to the applicable provisions in the Federal Acquisition Regulation to implement the recommendations provided pursuant to subsection (c)(i) of this section.

Sec. 4. Definitions. For purposes of this order, the following definitions shall apply:

(a) The term "bulk-power system" means (i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (ii) electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this order, this definition includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy.

(b) The term "bulk-power system electric equipment" means items used in bulk-power system substations, control rooms, or power generating stations, including reactors, capacitors,

substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems. Items not included in the preceding list and that have broader application of use beyond the bulk-power system are outside the scope of this order.

(c) The term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(d) The term "foreign adversary" means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or its allies or the security and safety of United States persons.

(e) The term "person" means an individual or entity.

(f) The term "procurement" means the acquiring by contract with appropriated funds of supplies or services, including installation services, by and for the use of the Federal Government, through purchase, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated.

(g) The term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 5. Recurring and Final Reports to the Congress. The Secretary is hereby authorized to submit recurring and final reports to the Congress regarding the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

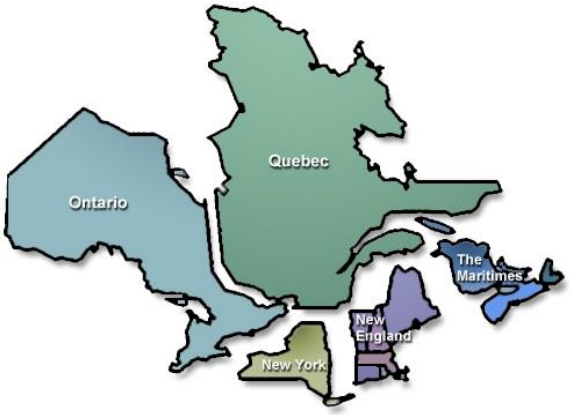
THE WHITE HOUSE,

NPCC, Inc.

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

DRAFT

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 12/XX/2020

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

Contributors

John Pearson	**ISO-NE**
Brad Marszalkowski	**ISO-NE**
David Forrest	**EPRI Consultant**
Ryan Quint	**NERC**
David Conroy	**Joint Utilities of New York-CMP**
Herb Schrayshuen	**Power Advisors on behalf of NextEra**
James Grant	**NYISO**
Brian Robinson	**Utility Services**
Dan Kopin	**Utility Services**
Michael Jones	**National Grid (RSC Co-Vice Chair)**
Quintin Lee	**Eversource (RSC Co-Vice Chair)**
Benjamin Loebick	**United Illuminating**
Guy V. Zito	**NPCC (RSC Chair)**

NPCC also thanks the Regional Standards Committee 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 and various enhancements and clarifications and Appendices**

Contents

Executive Summary 4
Introduction and Objective 5
NPCC DER Impact Reporting 7
DER BPS Impact Considerations 7
NPCC Interconnection Guidance 8
- Voltage Response 10
- Frequency Support 11
- Reconnection to the Utility System 12
- Inverters 12
- Certification per UL 1741 SA as grid support utility interactive inverters 13
- Minimum Protective Functions 14
- Metering 15
- Power Quality 17
- Power Factor 17
- Islanding 17
- Automatic Underfrequency Load Shedding (UFLS) Programs 17
- Effective Grounding for DER 18
- Resource Adequacy 18
- Energy Storage Systems for DER 19
- System control and Data Acquisition (SCADA) and Communications 20

DER Recommendations 20
Appendix A, NPCC DER Impact Reporting Form and Process 22
Appendix B, NPCC Areas- Comparisons 24
Appendix C – SPIDER Working Group Reliability Guidelines & Activities 25
Appendix D, NPCC Reliability Principles 28
Appendix E, State and Provincial AGIR Information 32
- New York State 32
- New England, by State 32
- Province of Quebec (some references are only available in French) 35
- Province of Ontario 38
- Province of New Brunswick 39

Appendix F, ISO New England 40

Appendix G, State Renewable and Green Energy Requirements 42

Commented [HS1]: Add a section on Resource Adequacy modelling after Effective GRounding

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 risks[1] to the BPS, recommendations to mitigate them, and also identifies opportunities to leverage the operational characteristics of DER to enhance reliability and resilience of the NPCC Bulk Power System (BPS). Helpful links to other resources are provided throughout the document.

As Distributed Energy Resources (DER) installed on the distribution system, 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"[2] 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 national efforts 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 are either developed, or in the process of being developed, by the NERC System Planning Impacts Working Group (SPIDER), along with links to some of their documents. NPCC and its members have been engaged in efforts at the national level and are leading efforts to address outstanding issues within the scope of those groups and provide expertise. With the understanding of what efforts are underway nationally, 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. Specifically, in the area of 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.

[1] 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,

[2] "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, analyze and determine a way to address any issues. 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 is purely informational and as NERC's SPIDER, 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 Labs, the Electric Power Research Institute 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 generating resources are included in DER is not broadly accepted by the industry. Also, DER is not currently a term that is defined by NERC.

For the purpose of this NPCC guidance, 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, irrespective of capacity, allowing individual small 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 would not include individual rooftop solar or wind turbines or other localized DER net metering installations, however the aggregate effect of these types of DER can have a significant change in 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 21[3]. NPCC is now observing aggregation of DER beginning to enter capacity wholesale markets within the NPCC Region. This document will continually 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 improvement and address potential reliability risks, promote good utility interconnection practices necessary for reliability, and promulgate

[3] 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 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.

information on how DER can enhance reliable operation of 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 as well as the Joint Utilities group of NY to align processes where possible.

National standards are established to address DER impact on system reliability. IEEE Std 1547-2018 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 through inclusion in those interconnection agreements.

As DER continues to penetrate 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 and influence the effect of these DER resources on the BPS. It is important to understand how DER is interconnected, planned, operated and how they interact with the transmission system.

Reliably and securely integrating DER into the electric system requires a comprehensive multi-pronged approach utilizing perspectives from different areas. 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 formulation 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 nature of the system within which 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 contemporary DER is theoretically capable of bringing several enhancements to reliability, provided that there are sufficient design specifications and interconnection requirements to implement the enhancements. Inverter based DER may use fast, programmable response to provide benefits to reliability if properly configured with coordination 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
- Under frequency 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.

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. EPRI has an open sourced co-simulation tool under test. 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.

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 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 reliablity issues and opportunities for further work, and provide general guidance and information where possible, offer consistent guidance with North America wide technical direction to promote reliable interconnection and operation of DER. It is recognized that DER may not be placed optimally and 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 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 availability and quality of forecasting.
- Observability and situational awareness of DER and importance of implementing Advanced Metering Infrastructure (AMI) if telemetry is not deployed
- DER impacts on Underfrequency Load Shed programs.
- Impacts of DER on the 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 others 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 guidance[4]. The level of detail and specificity provided is intended to be used as 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 are encouraged to reach out directly to other 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 for the simulated transmission event, the transmission system could become unreliable for that event and require remediation. This can occur in several scenarios such 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.

[4] At the time of this guidance document development, these include but are not limited to: NERC (e.g. SPIDER WG, IRPTF, Events Analysis, Modelling and Standards process), Inverter- Based Resources Task Force), IEEE (IEEE Std 1547-2018, P2800), and various state initiatives such as the New York ITWG, Other Regional, Provincial and State initiatives.

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 coordinate with NERC standard PRC-24-02. 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 ensuring a reliable transmission system at the lowest possible cost.

IEEE 1547-2018 was approved in 2019 and also unanimously adopted by the National Association of Regulatory Utility Commissioners (NARUC). The standard outlines the technical specifications and performance requirements which are universally needed for interconnection and interoperability of DER and will 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 the 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 and standards.

The DER owner must follow interconnection agreements and any AGIR requirements for fault ride through. Utilities and other AGIR entities should ensure that their requirements describe necessary DER performance with ride-through capabilities for frequency and voltage events. Interconnection agreements and standards generally have requirements to provide documentation upon request.

In terms of 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 standards 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 must be capable of automatically disconnecting the generation from the system to which it is directly connected upon detection of frequency or voltage conditions outside of the applicable ride-through requirements. Note that those interconnection agreements and standards should account for both distribution protection and reliability of the BPS. For three-phase installations, the over and under voltage function should be included for each phase and the over and under frequency protection on at least one phase. All phases of a generator or inverter interface should disconnect for appropriate voltage or frequency trip conditions sensed by the protective devices. Voltage protection should be wired phase to ground for single phase installations

and for applications using wye grounded-wye grounded service transformers. 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 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 Process[5].

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 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 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 band of voltage levels will ensure that DER do not prematurely trip and further deteriorate system conditions. IEEE Std. 1547-2018 includes ranges of 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.

[5] At this time there has not been an assessment of potential change in sensitivity (increase or decrease) to the effects of GMD from the presence of high DER penetration. This is a potential reliability risk to be evaluated in the future.

Quebec Interconnection

Ride through during system disturbances is of primary importance for resources connected to the grid, with the objective of maintaining system reliability[6]. 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 distribution resources 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. The sequence for a protective device to automatically initiate a disconnect sequence from the utility system is also detailed in the most current version of 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 is a need to establish a mechanism to ensure distribution provider transmit information to planners and operators as to which DER facilities are connected to distribution feeder that have UFLS protection systems.

Quebec Interconnection

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 DER must be capable of riding through frequency as low as 55.5 Hz (for a short time period). Therefore

[6] NERC report on Loss of Wind Turbines During System Disturbances : NERC Report-Loss of Wind Turbines

in Quebec, UFLS systems must operate outside this operating rang in accordance with the Quebec variance to the PRC-006-NPCC UFLS-1 regional standard table 4.

Reconnection to the Utility System

If the generation facility is disconnected as a result of the operation of a protective device, the DER owner's equipment must 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.

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, 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 changes direct current (DC) to alternating current (AC). The inverter itself does not produce any 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 bands for voltage ride-through capabilities that are attainable by inverter-based systems where there 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 EPS and to provide increased BPS reliability by further reducing the potential loss of DER during bulk system events.

Inverters intended to provide local grid support during system events that result in voltage and/or frequency excursions as described in this document and should be provided with the required onboard 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 standards and agreements also typically refer to IEEE Std. 1547-2018 functional requirements and include protection setting review requirements.

ISO-NE also has developed a technical bulletin, contained in **Appendix F**, which outlines required settings for inverters in New England.

Certification per UL 1741 SA as grid support utility interactive inverters

Because Inverters certified for IEEE 1547-2003 do not currently provide adequate grid support functionality, in the interim period while IEEE P1547.1-2018 is not yet revised and published, 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. 1547-2018 (2nd ed.)1 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.
- Abnormal performance capability (ride-through) requirements for inverter-based applications should have the ride-through capability per abnormal performance Category II of IEEE Std. 1547-2018 (2nd ed.) as quoted in Tables III and IV. Additionally, an effort is underway at IEEE to

amend 1547-2018 to expand the range of under-voltage trip settings in Category III. If the amendment is approved, Category III inverters should be recommended for use.

Minimum 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 distributed generation facility

• Voltage level of the interconnection

• Location of the distributed generation facility on the circuit

• Distribution transformer

• Distribution system configuration

• Available fault current

• Load that can remain connected to the distributed generation facility under isolated conditions

• Amount of existing distributed generation 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 will 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 the generating equipment.

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 DG 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)[7]. 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.

[7] 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.

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.

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). Net Energy Metering should be required when a DER has the capability or potential to provide generation back into the utility distribution system, however, the eligibility of a DER provider to receive net metering will be subject to the rules of the interconnecting utility and the local regulatory authority that has jurisdiction.

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. 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 reliably 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

The requirements for acceptable flicker levels should be in accordance with the latest version of IEEE Std. 1453 Recommended Practice for the Analysis of Fluctuating Installations on Power Systems. Short and long-term perception of flicker should be within the planning and compatibility levels delineated in any applicable requirements or standards.

Power Factor

If the output power factor, as measured at terminals of the generator, does not meet the connecting utility's power factor requirements, the method of power factor correction necessitated by the installation of the generator can be negotiated with the utility as a commercial item. If the average power factor of the DER over time is proven to be outside 0.9 (leading or lagging) by the customer and accepted by the utility, that power factor range may be used for any further utility facility design calculations and requirements.

Induction power generators may be provided with a VAR capacity from the utility system. The installation of VAR correction equipment by the generator- owner on the DER owner's side of the PCC is to be reviewed and approved by the interconnecting utility prior to installation.

Islanding

The guidance provided in this document is designed and intended to avoid islanding and may be superseded by local requirements. Additional protection schemes and system modifications may be necessary based on the capacity of the proposed system and the configuration and existing loading on the subject circuit.

The need for zero sequence voltage and direct transfer trip protection schemes should be evaluated based on minimum loads on the associated feeder and substation bus, including the impact of fault conditions resulting from DER installation to protect facilities for an islanded condition.

Transfer trip is needed in some instances (e.g. on DER connections to non-radial transmission or sub-transmission circuits) in order to protect the utility systems and DER facility from damage during faults and/or reclosing operations into faults. The decision as to the applicability of direct transfer trip and specific technology to be used form direct transfer trip communications rests with the connecting utility.

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 control operation designed to stabilize BPS islands for a generation deficiency. Various fractions of load are shed through this process, typically 25%. UFLS is primarily installed on distribution feeders, where DER is increasingly being deployed.

NERC has a set of requirements in the PRC-006 standard and NPCC has more stringent requirements in NPCC's Regional Standard, PRC-006-NPCC 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

With the onset of high penetrations of DER, such as photovoltaic (PV) generation, utilities should consider interconnection of PV plants 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 plants are considered voltage-controlled current sources during faults. Inverter-based plants generally provide less short-circuit current than similarly sized synchronous unit.

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.

Resource Adequacy

Forecasting resource adequacy is an import system reliability function. The reporting of generation capability and 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 planners and system operators. Any requirements associated with this information should be in Interconnection Agreements or Tariffs prior to any commissioning of the DER. There are currently no mechanisms within NERC Standards or NPCC Criteria to require DER entities to provide this information. It currently needs to be covered under other contractual agreements such as local utility Interconnection Agreements or Tariffs.

Commented [HS2]: I put this here as a placeholder. More can be said if needed.

Energy Storage Systems for DER

Battery storage technology is undergoing a rapid evolution from Lead Acetate 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 "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 below, the capability of an inverter can be exceeded by the capability of the DER behind it. This is designed with due consideration of the degradation of DER, such as a solar panel over time.

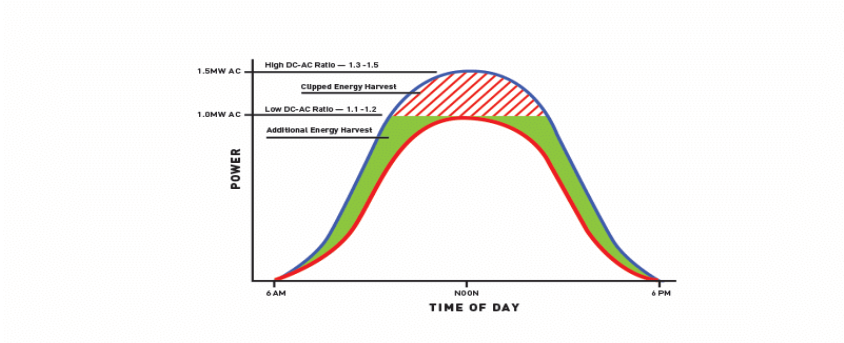


Figure 1- Storage showing Clipped and Unused Energy

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 emergent or planned outage situations. Some NPCC Members have encountered difficulty with obtaining information and data from the DER. 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. 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.

DER Recommendations

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

Participation in National DER Forums

1) Participate in national efforts to fully understand the issues and best practices associated with DER.
2) Engage NPCC and its members at the national level leading efforts to address the issues and provide expertise.
3) As the understanding at the national level 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 generating resources, 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 problem 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 stakeholder.
9) Avoid placement of UFLS on distribution feeders with DER unless sufficient telemetry exists to ensure proper functionality of the UFLS program as a whole.

<u>Planning Related Recommendations Due to Changing Resource Mix</u>

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 BPS[8]
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.

<u>Analytics and simulation recommendations to deal with increase system complexity</u>

10) Support interconnection wide inertia loss study efforts, to determine potential reliability impacts, as DER replaces conventional synchronous generation resources.
11) 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.

[8] 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.

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 to; npccstandard@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.

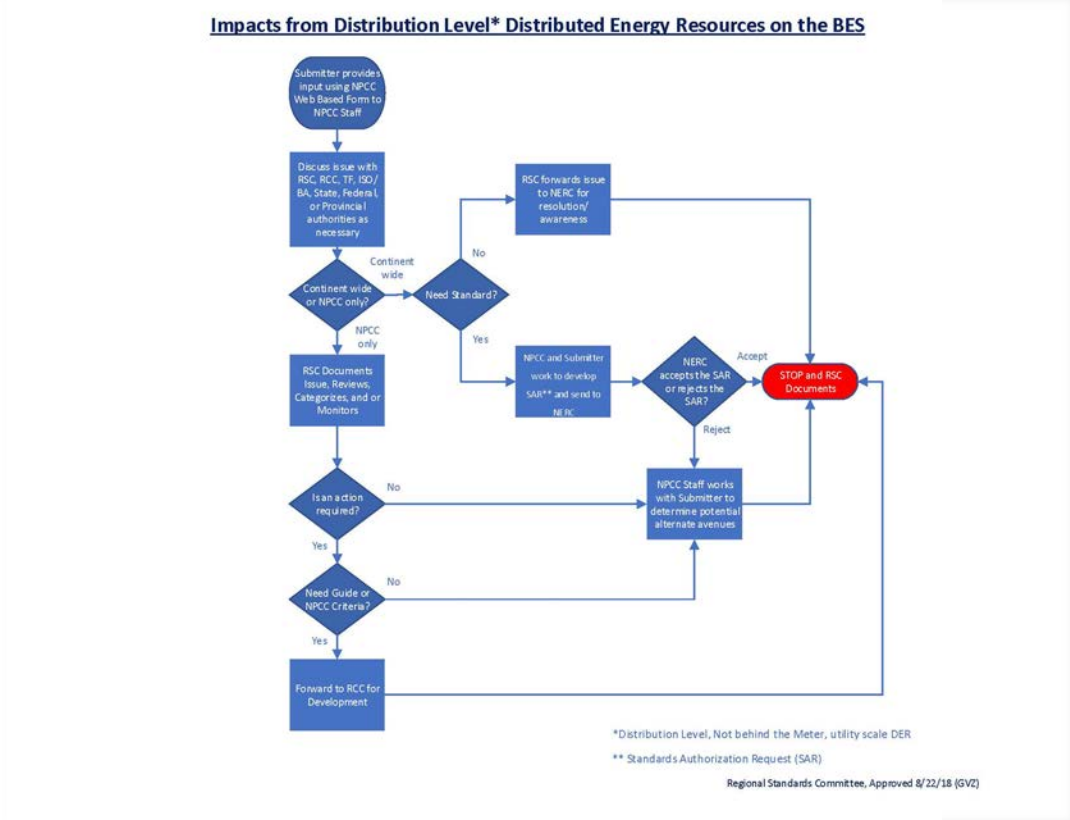
Root Cause or additional Analysis

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



Appendix B, NPCC Areas-Comparisons

Key Inverter based specification extracts

	ISO-NE Inverter Requirements	NG ESB 756 B, C, D	NY SIR[9]	IESO F2 Technical Requirements

[9] NY SIR is the New York Standardized Interconnection Requirement.

Inverter Certification	yes	yes	yes	yes
Voltage and frequency trip settings for inverter-based applications	yes	yes	yes	yes
Voltage Response	yes[10]	yes	yes	yes
Frequency Response	yes[11]		yes	yes
Abnormal performance capability (ride-through) requirements for ~~inverter based~~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	

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

[10] 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

[11] 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

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"[12]:

> **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.

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)

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

	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 Criteria[13], 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

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

requirements. NPCC's core Reliability Principles[14] 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 region[15]. These critical facilities collectively are identified as the NPCC Bulk Power System[16,17].
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 operation[18] 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 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."

[14] The Reliability Principles were summarized in the NPCC 2018 Strategic Review Report.
[15] 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.
[16] 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.
[17] 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
[18] 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. "

6. **Resilience has always been an element of NPCC Criteria:** Based on experience, resilience[19] [20] 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

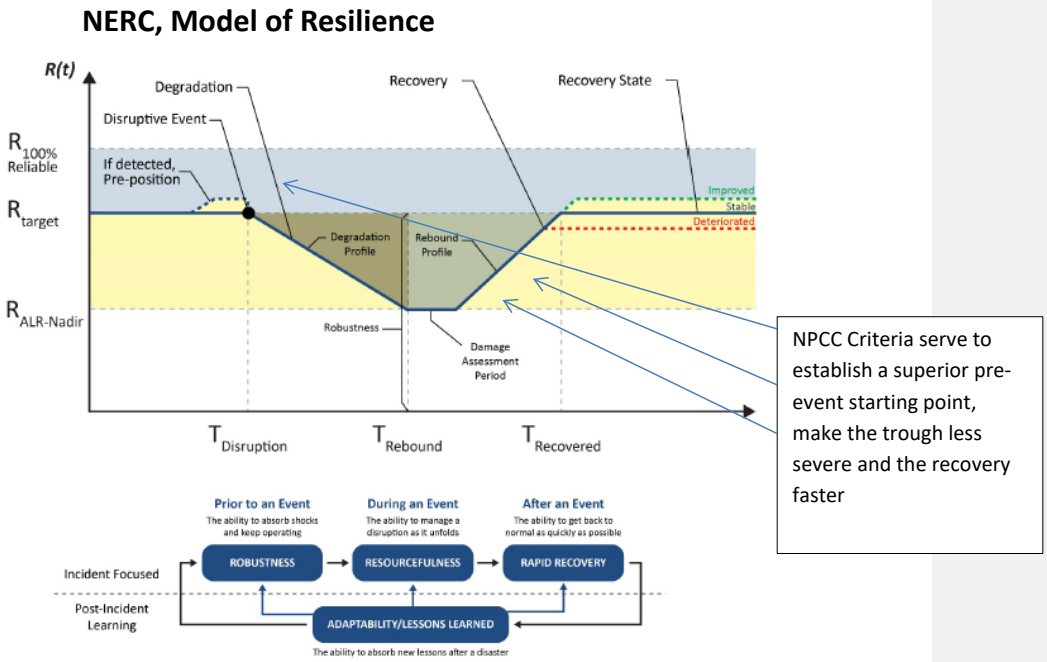


Figure 2.1

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

[19] 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.
[20] In 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".

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 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 (HQCMÉ) 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.

We know you also contacted Hydro-Québec in this matter, but just in case, 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

As noted above, 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

Ènergie 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 (2nd ed.) Category II					
Shall Trip Function	Required Settings		Comparison to IEEE Std 1547-2018 (2nd 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 (2nd 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 (2nd ed.) for Category II
V > 1.20	Cease to Energize	N/A	0.16	Identical
1.175 < V ≤ 1.20	Permissive Operation	0.2	N/A	Identical
1.15 < V ≤ 1.175	Permissive Operation	0.5	N/A	Identical
1.10 < V ≤ 1.15	Permissive Operation	1	N/A	Identical

0.88 ≤ V ≤ 1.10	Continuous Operation	infinite	N/A	Identical
0.65 ≤ V < 0.88	Mandatory Operation	Linear slope of 8.7 s/1 p.u. voltage starting at 3 s @ 0.65 p.u.: $T_{VRT} = 3\text{ s} + \frac{8.7\text{ s}}{1\text{ p. u.}}(V - 0.65\text{ p.u.})$	N/A	Identical
0.45 ≤ V < 0.65	Permissive Operation [a,b]	0.32	N/A	See footnotes a & b
0.30 ≤ 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:

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

b. 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 (2nd ed.) for Category II
f > 62.0	No ride-through requirements apply to this range		Identical
61.2 < f ≤ 61.8	Mandatory Operation	299	Identical
58.8 ≤ f ≤ 61.2	Continuous Operation	Infinite	Identical
57.0 ≤ 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 Requirements

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

EPRI T&D Research Related to DER Integration

Devin Van Zandt, dvanzandt@epri.com
Jens Boemer, jboemer@epri.com

NPCC DER Forum Webinar

May 14, 2020



This presentation is, in part, supported by the U.S. Department of Energy, Solar Energy Technologies Office under Award Number DE-EE0009019 *Adaptive Protection and Validated MODels to Enable Deployment of High Penetrations of Solar PV (PV-MOD).*

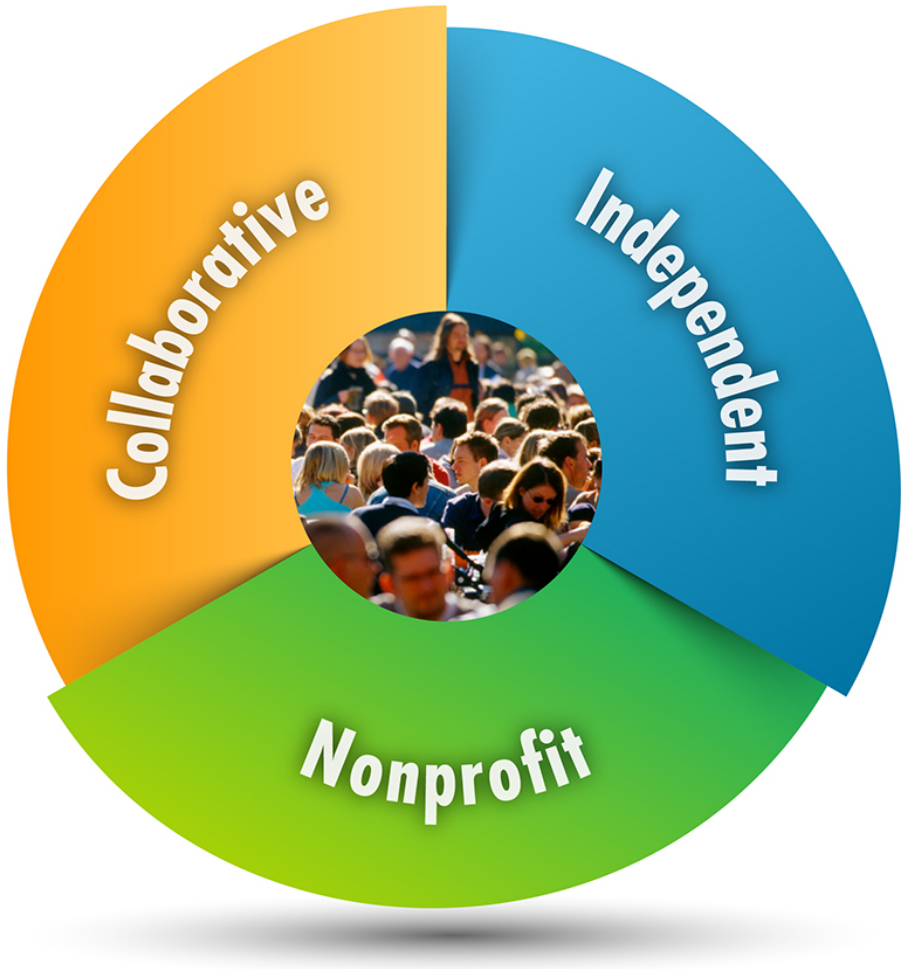
© 2020 Electric Power Research Institute, Inc. All rights reserved.

Presentation Outline

- EPRI T&D Research
- EPRI COVID-19 Impacts Review
- Distribution System Topics
- Transmission System Topics
- Q&A

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Three Key Aspects of EPRI



Independent

Objective, scientifically based results address reliability, efficiency, affordability, health, safety, and the environment

Nonprofit

Chartered to serve the public benefit

Collaborative

Bring together scientists, engineers, academic researchers, and industry experts

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Our Members...

- 450+ participants in more than 30 countries
- EPRI members generate approximately 90% of the electricity in the United States
- International funding – nearly 25% of EPRI's research, development, and demonstrations













© 2020 Electric Power Research Institute, Inc. All rights reserved.

Integrated Grid & Energy Systems

Strategic Energy & Env Planning

Long-Term System Planning

Real-Time Operations

Corporate Strategy and Integrated Resource Planning

System Protection

Strategic Planning

Technology Assessment

Resource Adequacy

Trans & Dist Planning

Renewable Integration

Operations Planning

Real-Time Operations

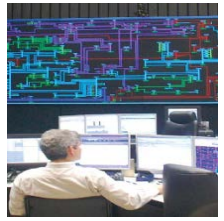
Market Operations & Design

Energy, Environment & Climate Policy



Integrated Energy System Planning, Fuels & Markets

Transmission Operations





Transmission Planning

Bulk System DER & Renewables Integration





Distribution Operations & Planning

Distributed Energy Resource Integration



Energy Storage Systems Integration

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Impact on Demand of COVID-19 Shutdown

Email any insights related to COVID-19 on electricity systems to our confidential inbox: covid19-grid-impact@epri.com

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Information and disclaimers about analysis

- **US and European Analysis based on publicly available data from ENTSO-E and EIA**:
  - https://transparency.entsoe.eu/ (account needed to download)
  - https://www.eia.gov/opendata/
  - Other countries based on data provided to us directly

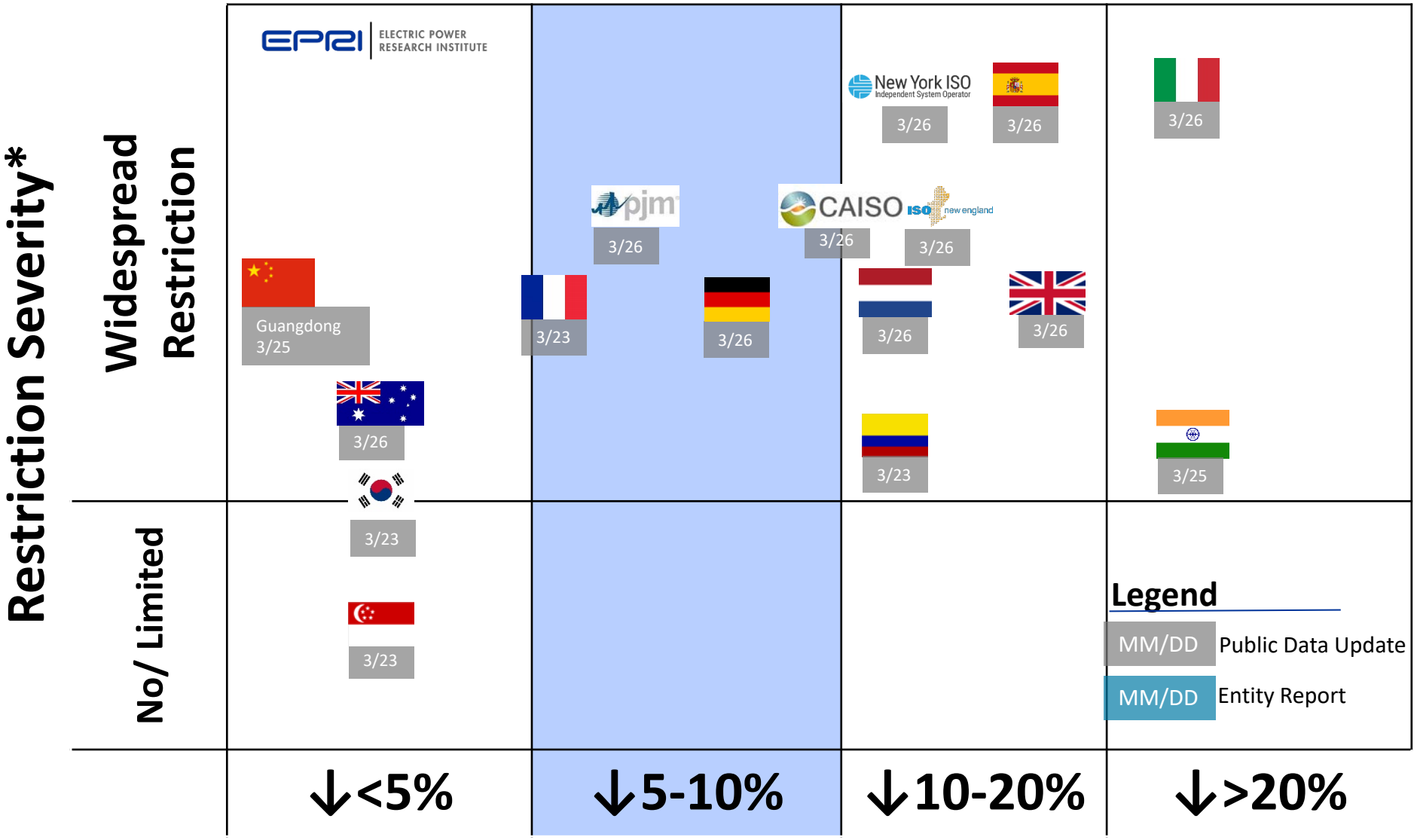
- **Other factors are not considered but likely to impact load levels**
  - Temperature
  - Behind-the-meter resources, etc.
  - Underlying, non-COVID economic factors

- **EPRI continues to monitor and update this information**
- **Public Report Available: https://www.epri.com/#/pages/product/3002019435/**

© 2020 Electric Power Research Institute, Inc. All rights reserved.

COVID-19 Demand Impact Classification

Effective: Mar 27th



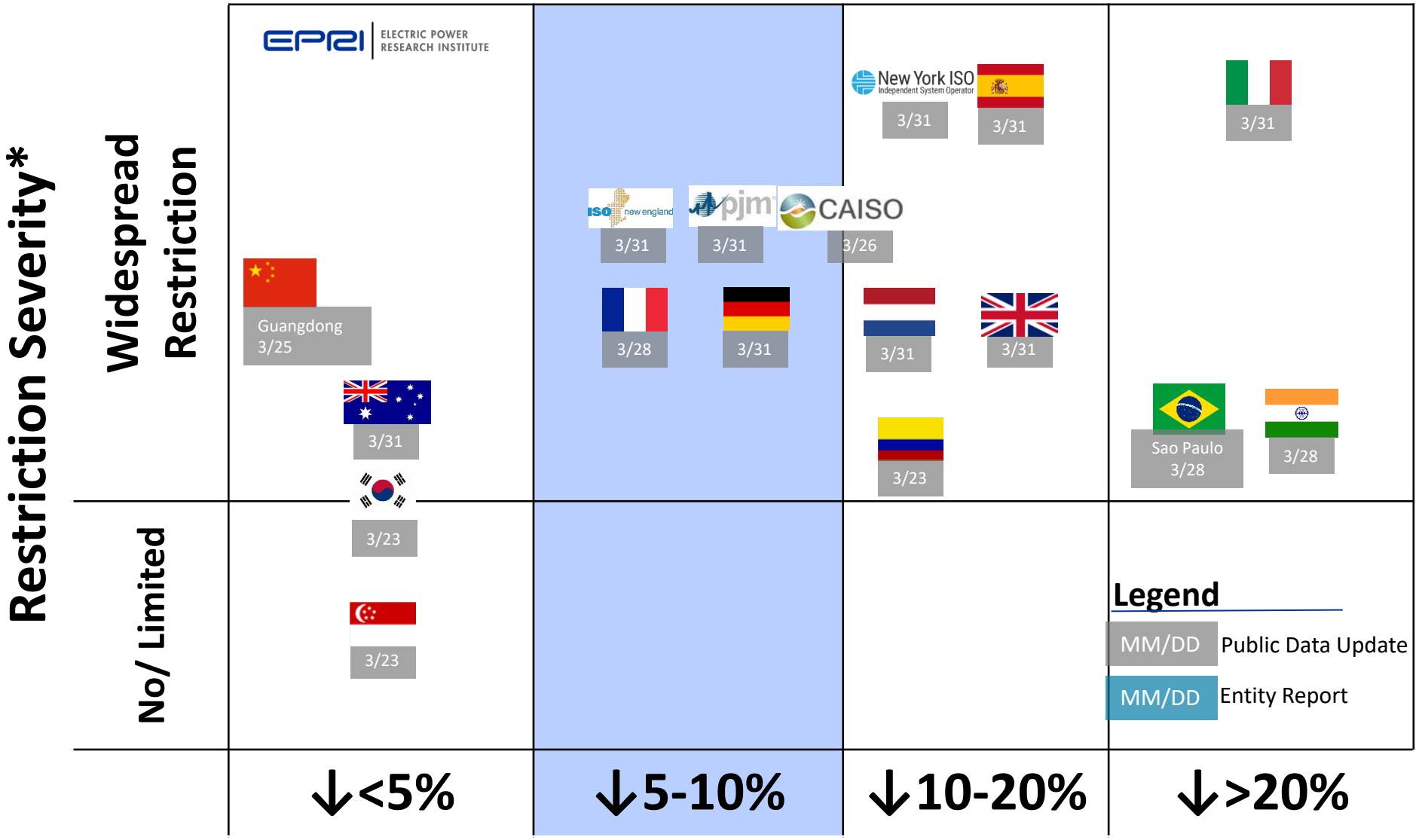
Data Sources: ENTSO-E, EIA, POSOCO, EMC, data.gov.kr, XM, bjx.com.cn, RTE, ISA, Transgrid, AEMO, CAISO, PJM

*Restriction severity varies substantially from region to region. Classification based on media reported restrictions

© 2020 Electric Power Research Institute, Inc. All rights reserved.

COVID-19 Demand Impact Classification

Effective: Mar 31st



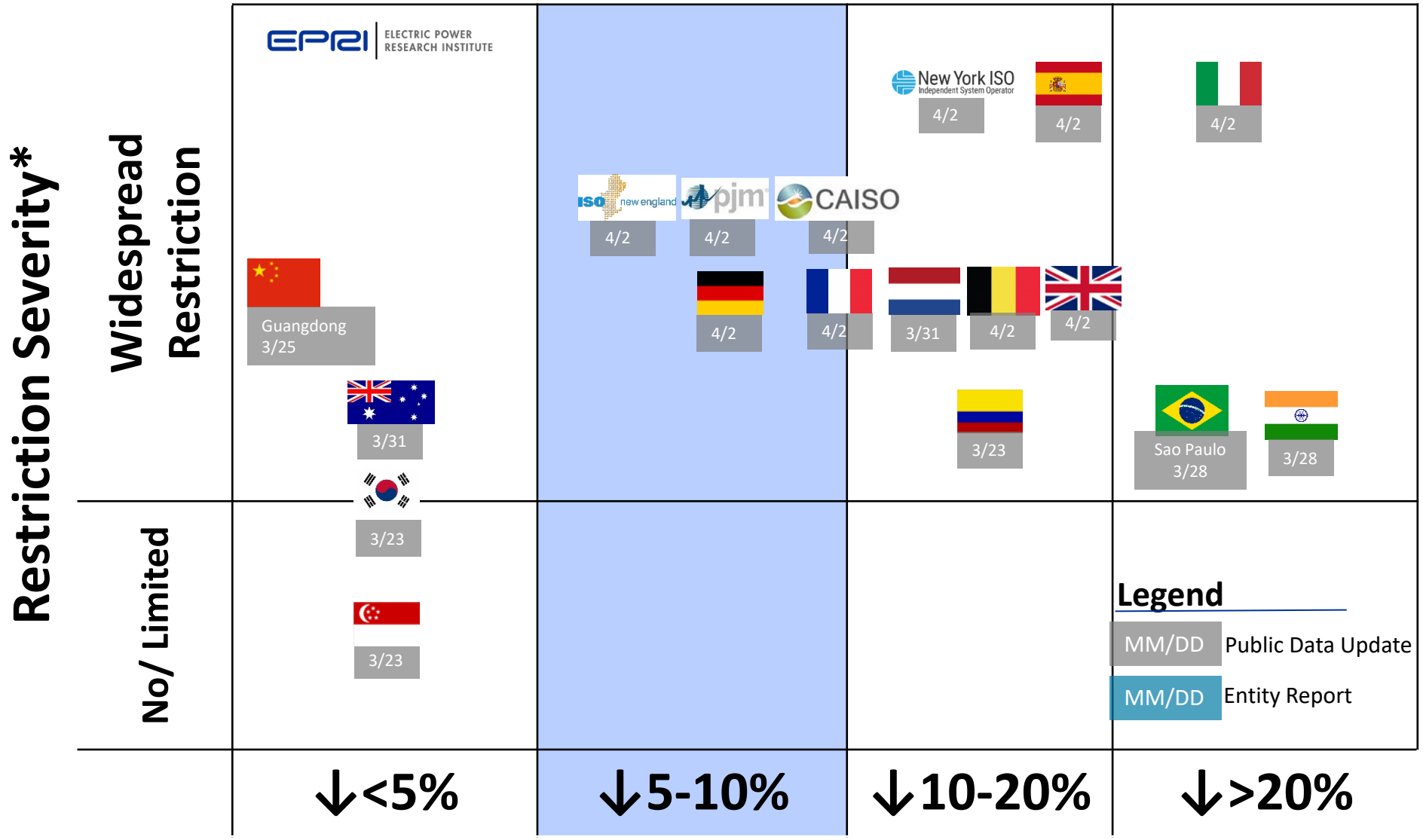
Data Sources: ENTSO-E, EIA, POSOCO, EMC, data.gov.kr, XM, bjx.com.cn, RTE, ISA, Transgrid, AEMO, CAISO, PJM

*Restriction severity varies substantially from region to region. Classification based on media reported restrictions

© 2020 Electric Power Research Institute, Inc. All rights reserved.

COVID-19 Demand Impact Classification

Effective: Apr 3rd



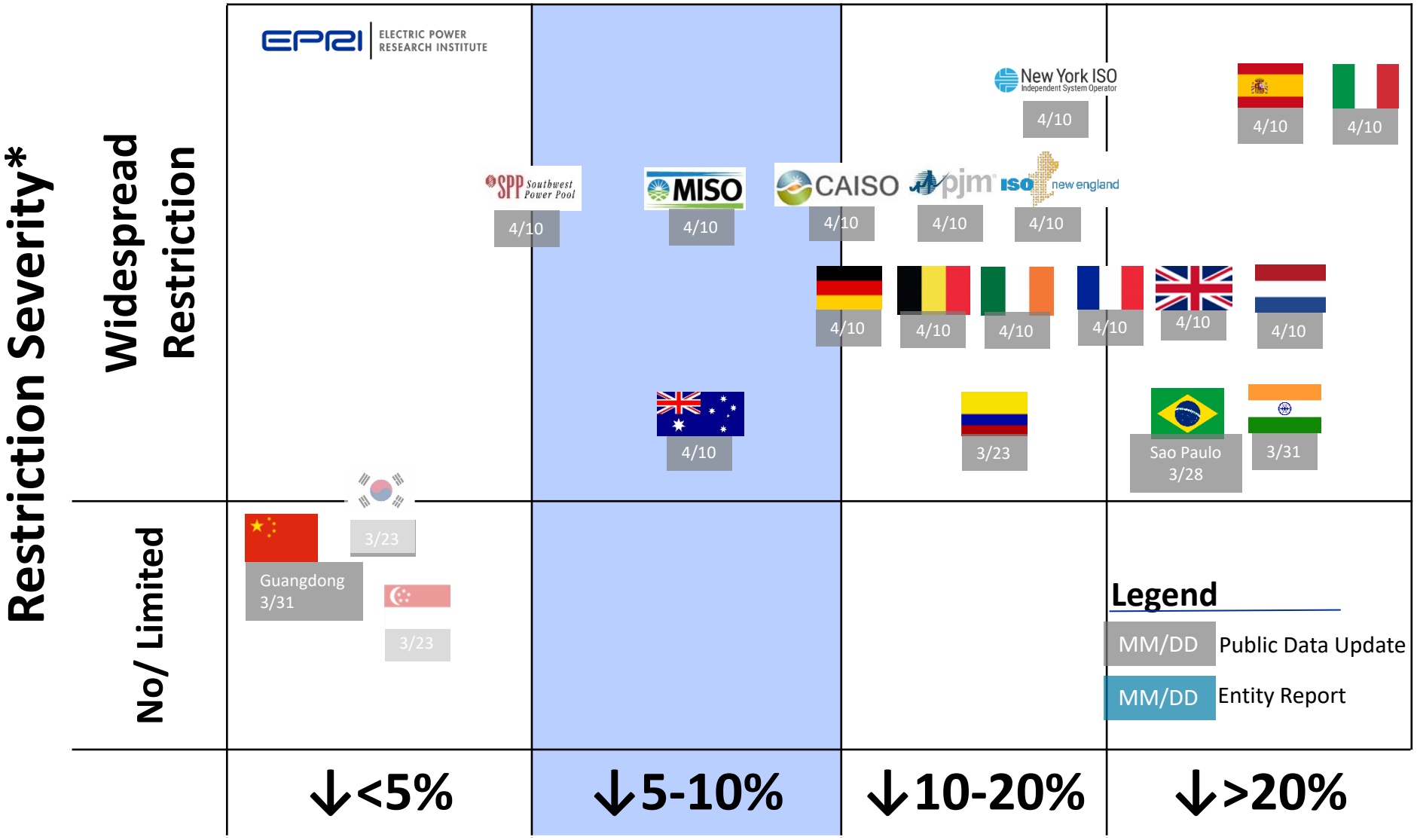
Data Sources: ENTSO-E, EIA, POSOCO, EMC, data.gov.kr, XM, bjx.com.cn, RTE, ISA, Transgrid, AEMO, CAISO, PJM

*Restriction severity varies substantially from region to region. Classification based on media reported restrictions

© 2020 Electric Power Research Institute, Inc. All rights reserved.

COVID-19 Demand Impact Classification

Effective: Apr 10th



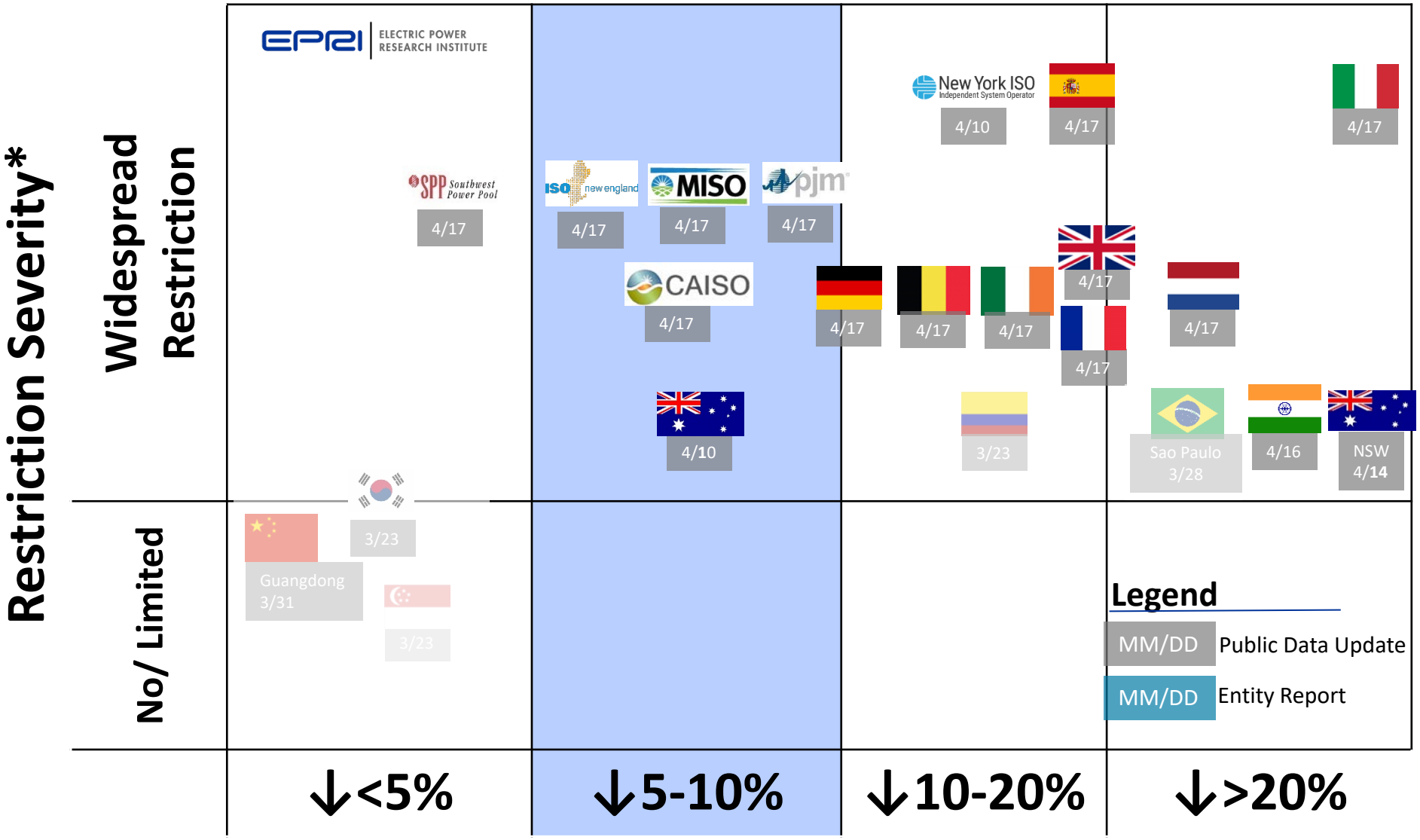
Data Sources: ENTSO-E, EIA, POSOCO, EMC, data.gov.kr, XM, bjx.com.cn, RTE, ISA, Transgrid, AEMO, CAISO, PJM

*Restriction severity varies substantially from region to region. Classification based on media reported restrictions

© 2020 Electric Power Research Institute, Inc. All rights reserved.

COVID-19 Demand Impact Classification

Effective: Apr 17th



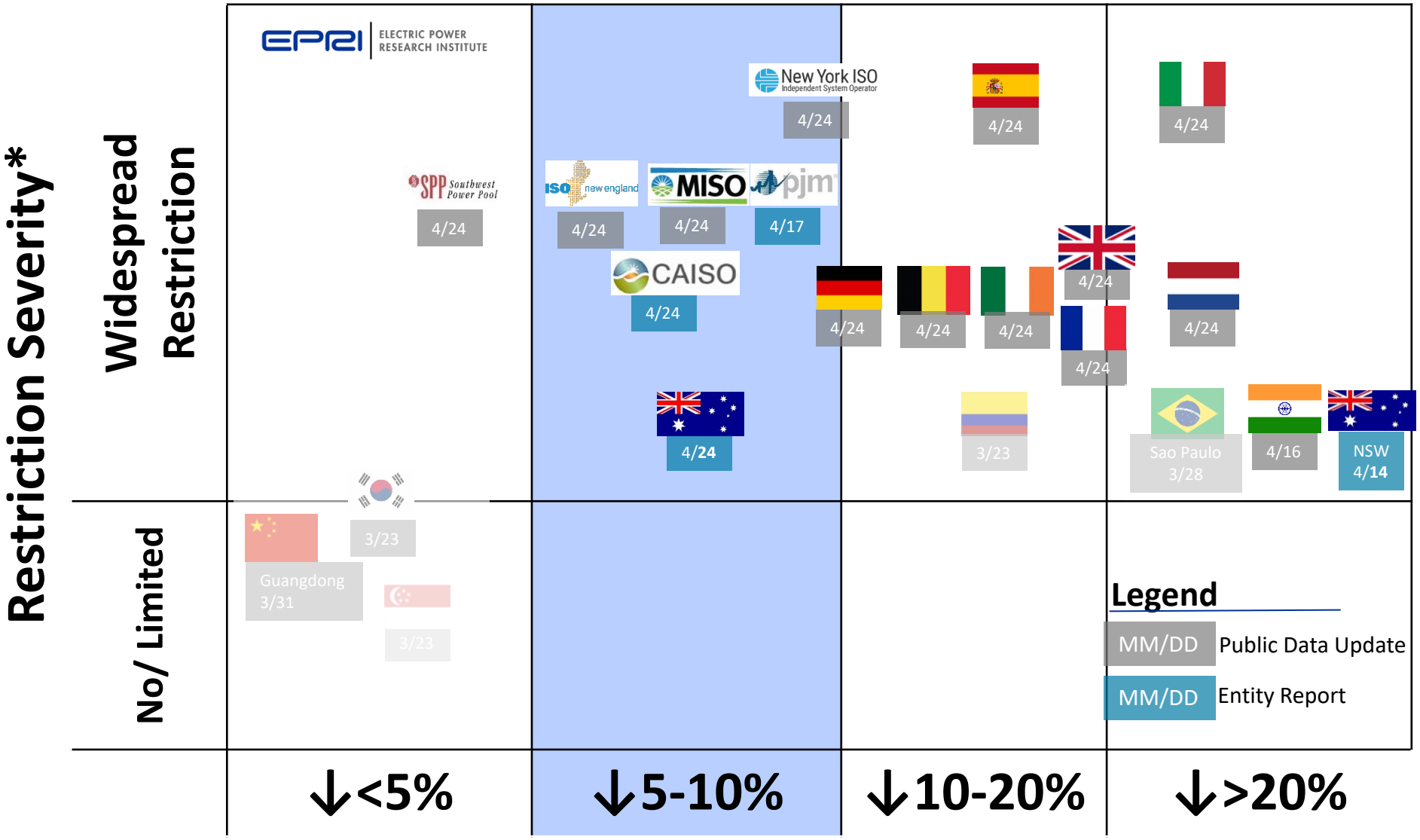
Data Sources: ENTSO-E, EIA, POSOCO, EMC, data.gov.kr, XM, bjx.com.cn, RTE, ISA, Transgrid, AEMO, CAISO, PJM

*Restriction severity varies substantially from region to region. Classification based on media reported restrictions

© 2020 Electric Power Research Institute, Inc. All rights reserved.

COVID-19 Demand Impact Classification

Effective: Apr 24th



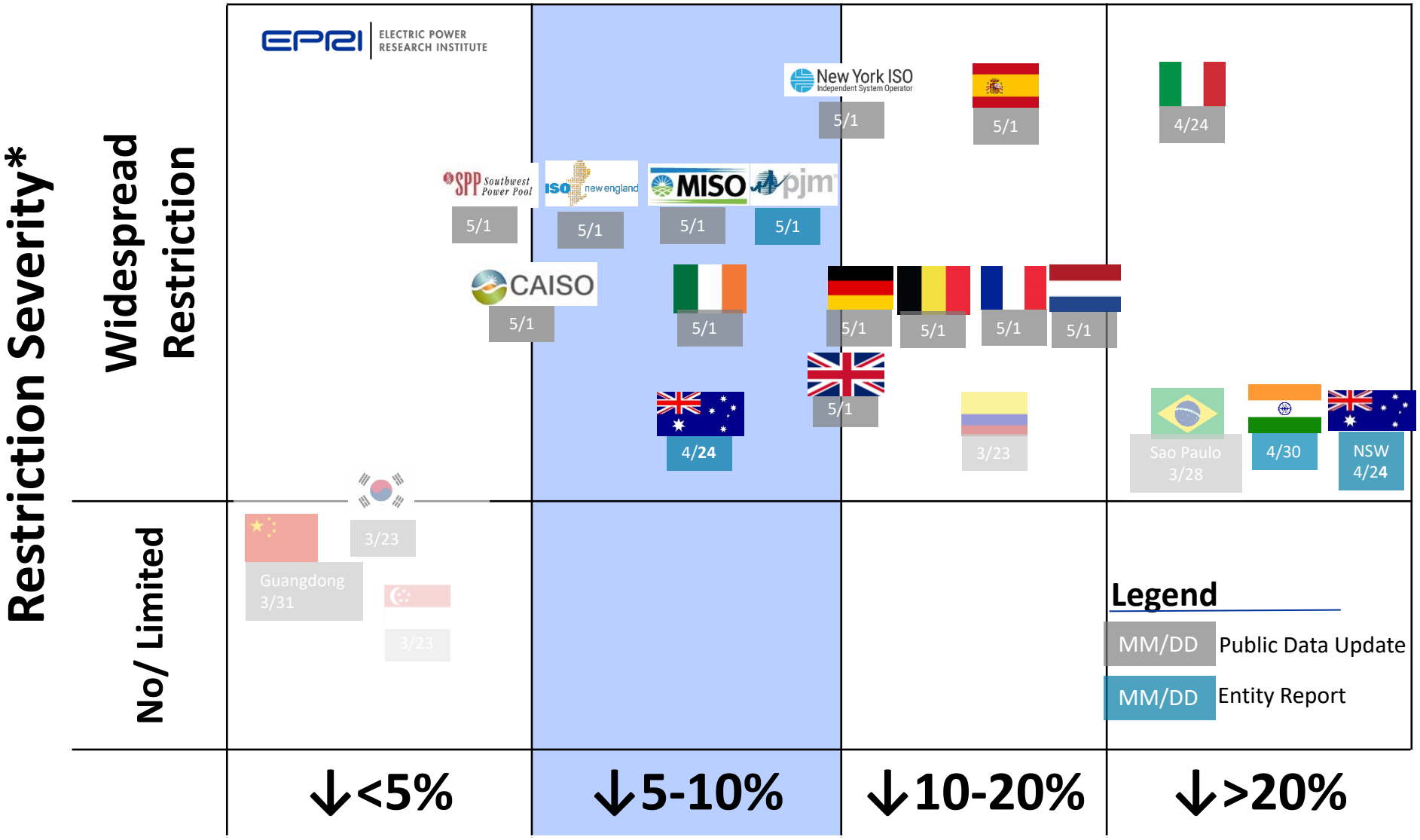
Data Sources: ENTSO-E, EIA, POSOCO, EMC, data.gov.kr, XM, bjx.com.cn, RTE, ISA, Transgrid, AEMO, CAISO, PJM

*Restriction severity varies substantially from region to region. Classification based on media reported restrictions

© 2020 Electric Power Research Institute, Inc. All rights reserved.

COVID-19 Demand Impact Classification

Effective: May 1st



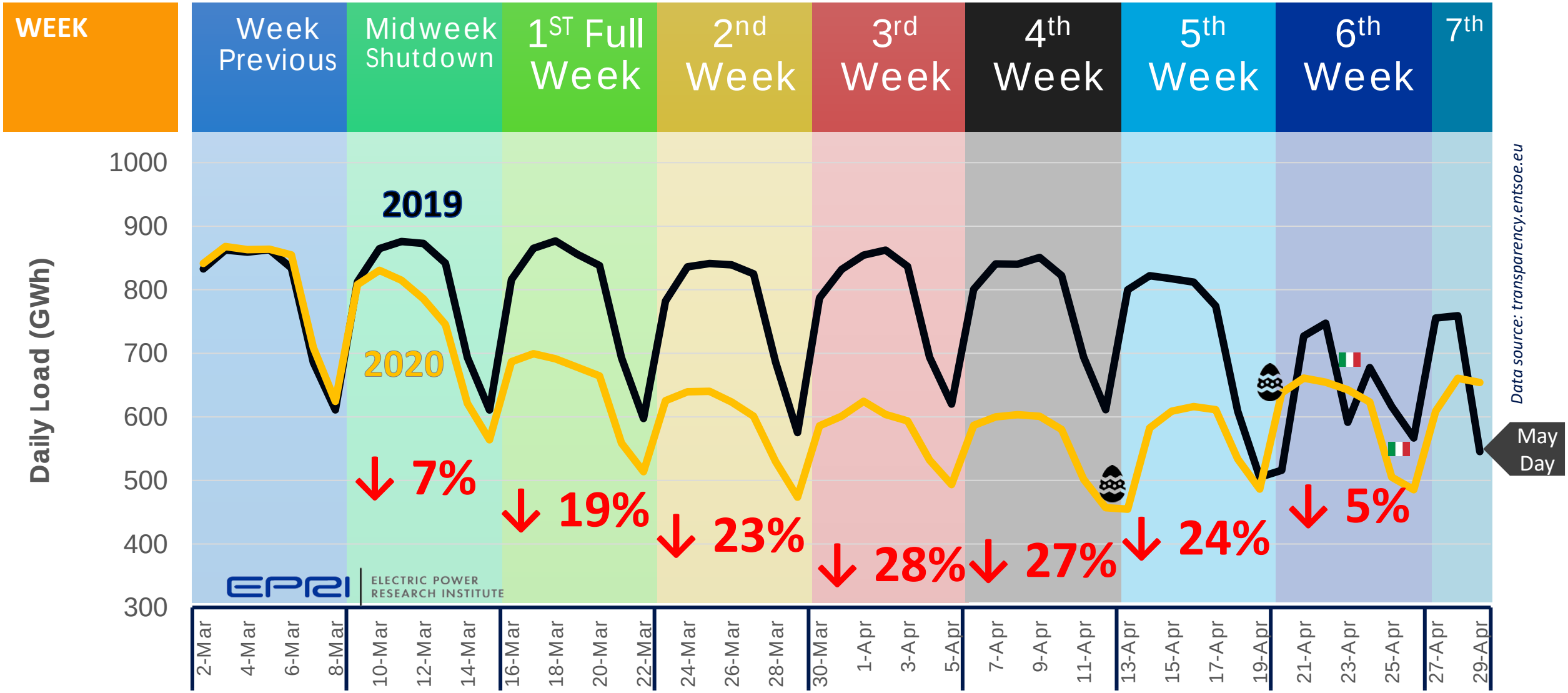
Data Sources: ENTSO-E, EIA, POSOCO, EMC, data.gov.kr, XM, bjx.com.cn, RTE, ISA, Transgrid, AEMO, CAISO, PJM

*Restriction severity varies substantially from region to region. Classification based on media reported restrictions

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Italian Electricity Demand – 2019 vs 2020

Italia



Data source: transparency.entsoe.eu

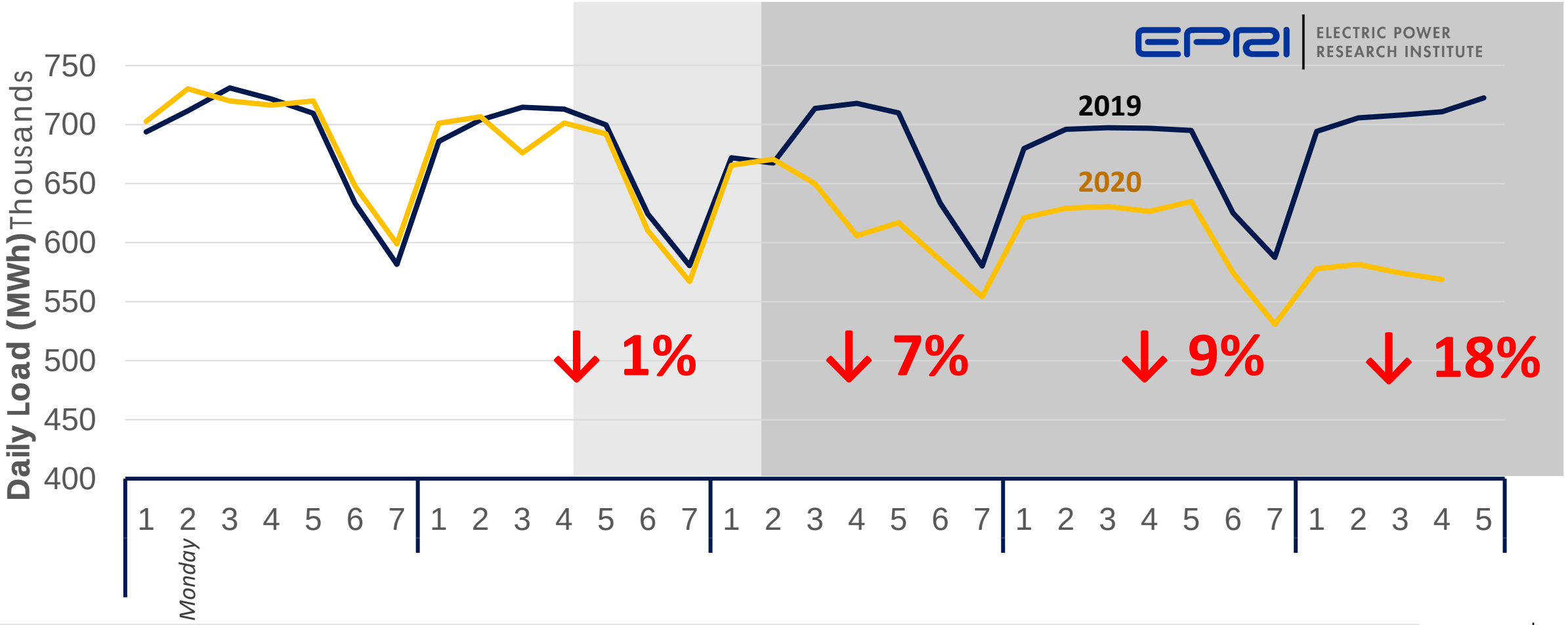
Weather and economic growth impacts not considered but clear trend observable

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Spanish Load in First 4 Weeks - 2019 vs 2020

España

PHASE	Week Previous	Midweek Shutdown	First Full Week	Second Full Week	Third Week



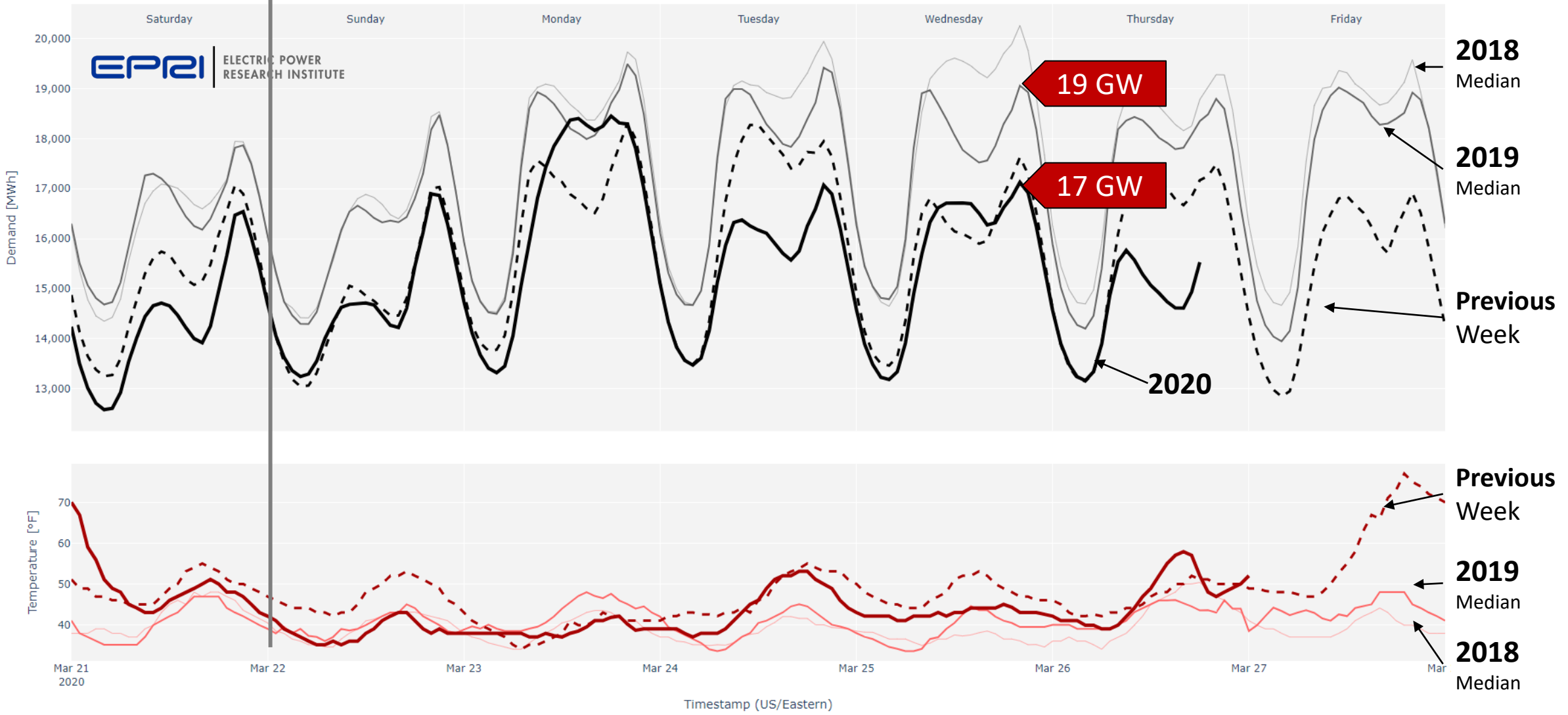
Data Source: transparency.entsoe.eu

© 2020 Electric Power Research Institute, Inc. All rights reserved.

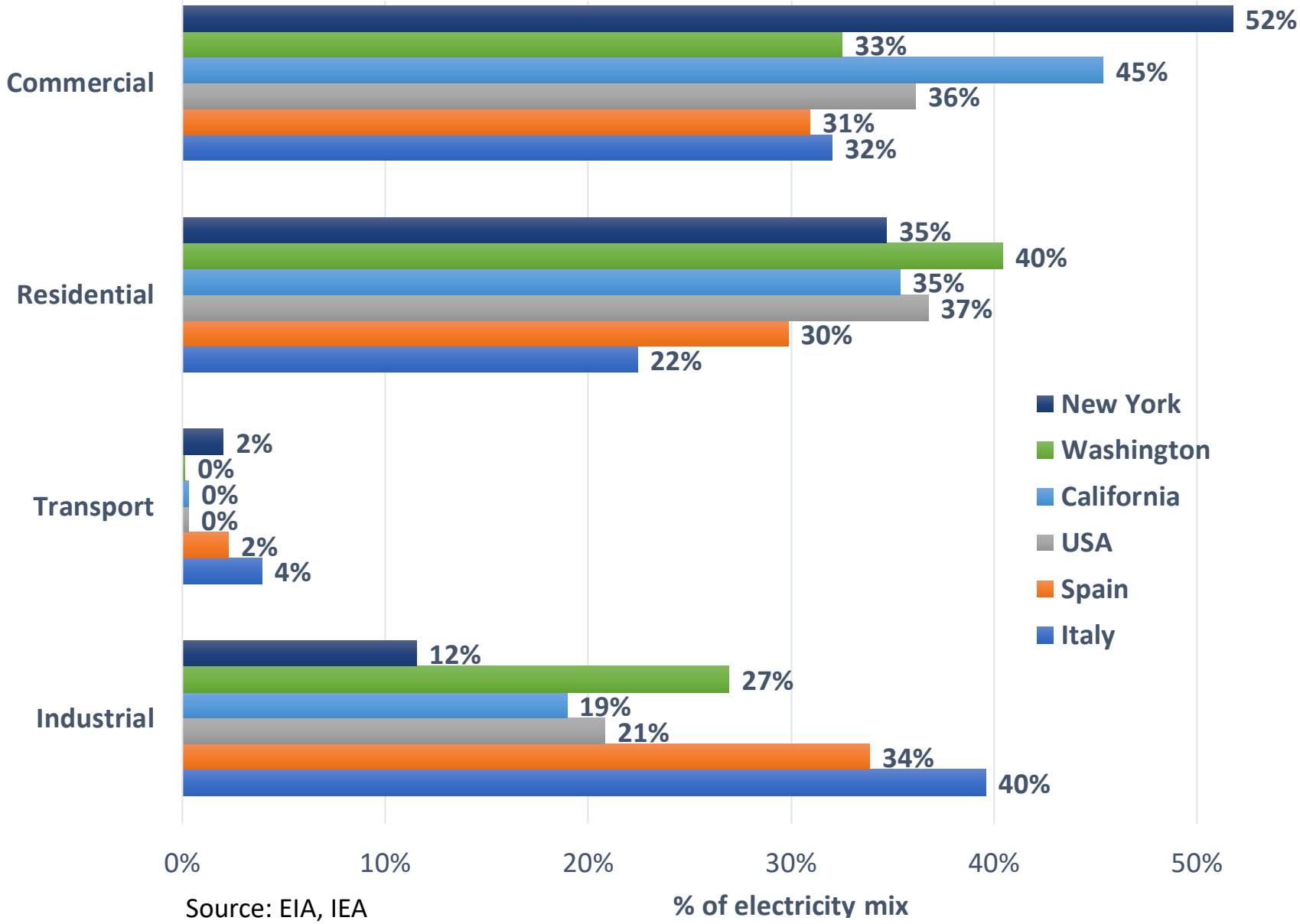
NYISO Load Over Past Week and Previous

New York ISO
Independent System Operator

Full Lock Down



Comparison: Electricity Consumption Mix



Source: EIA, IEA

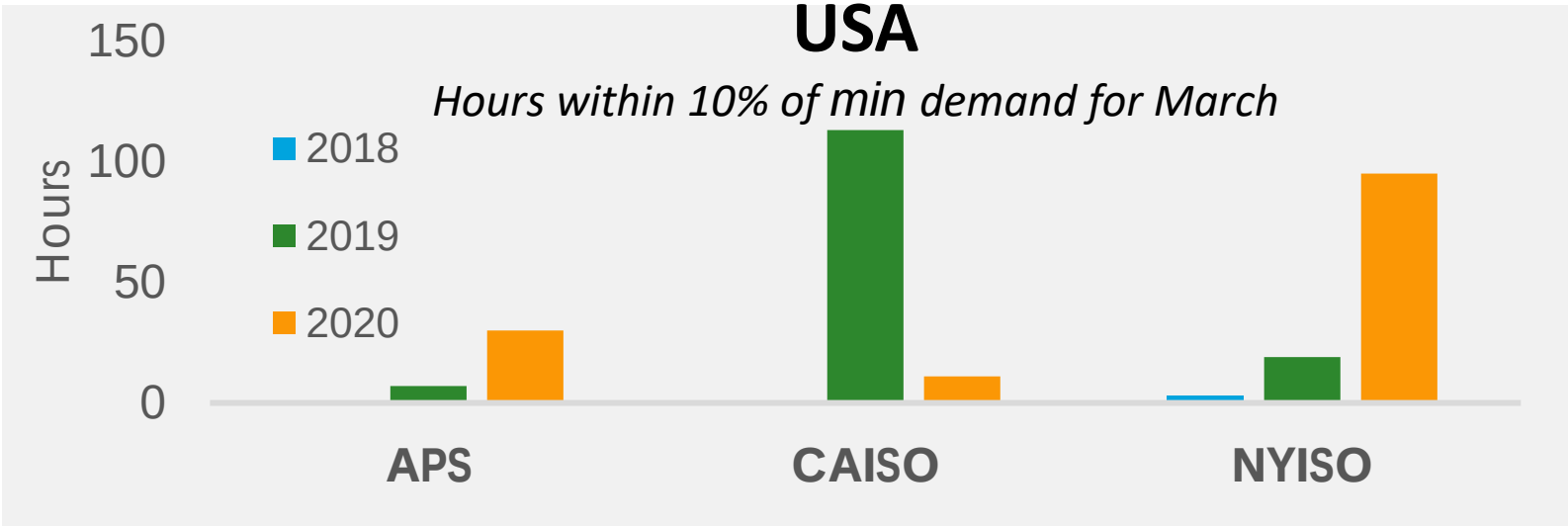
Commercial similar across Italy, Spain, and U.S, but higher in CA and NY.

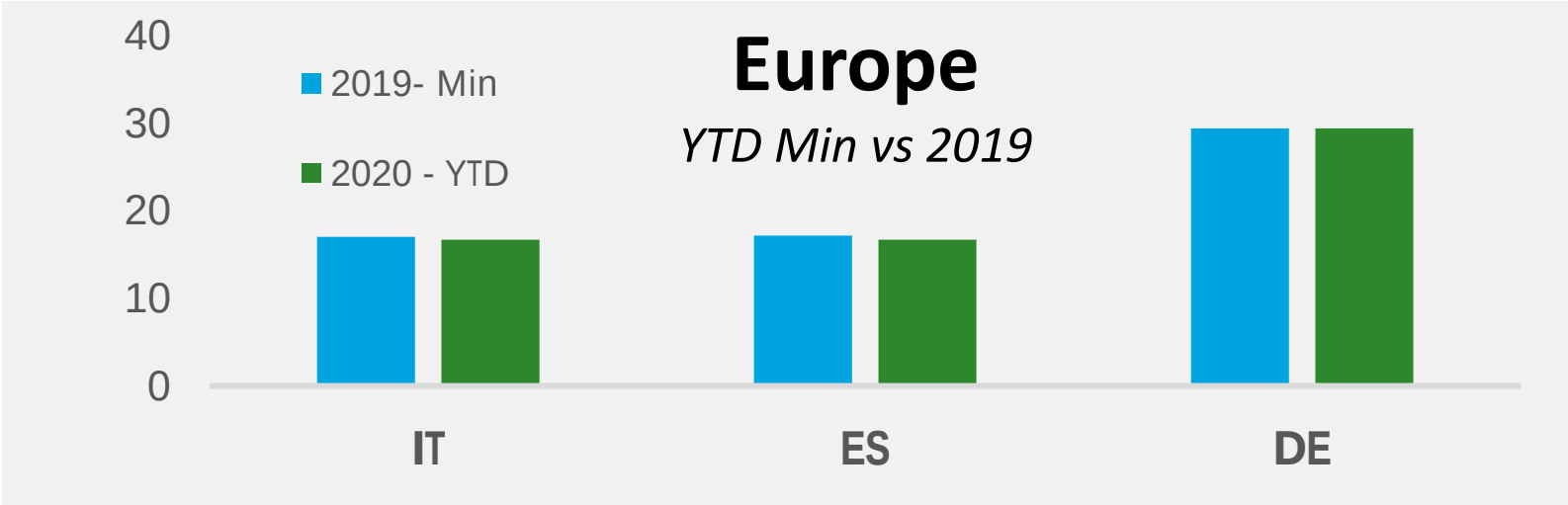
Residential lower in Italy.

Industrial higher in Italy and Spain; may result in greater impact

Annual and Monthly Min. Demands Records

- Several systems seeing record low minimum daily demands in US and Europe
- **78%** of extreme low demand periods in **NYISO** in March were **during day time**
- Issue **not** observed in CAISO thus far

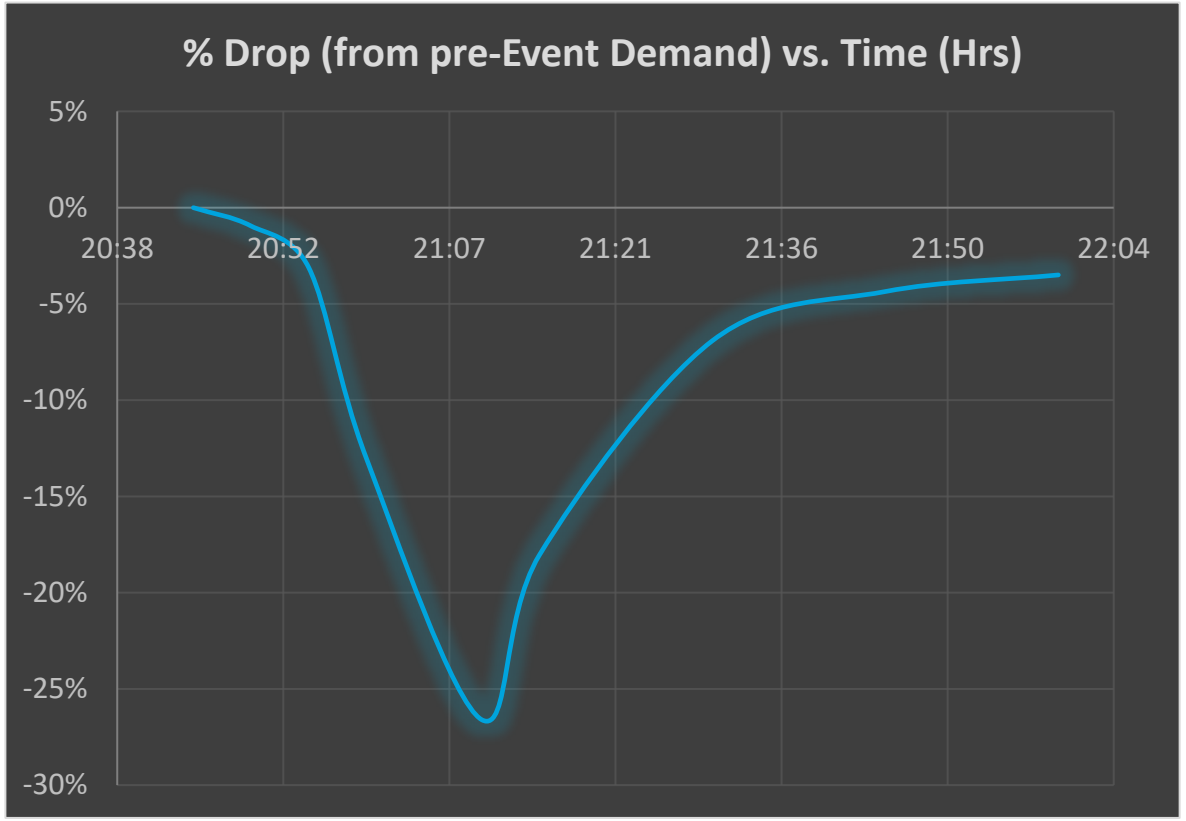




© 2020 Electric Power Research Institute, Inc. All rights reserved.

Indian April 25th Ramp Event

- Prime Minister of India appealed to the citizens on to switch off their 5th April at 21:00 for 9 minutes
- Notice issued on **April 3rd 9 AM**
- Anticipated change in load: 11-14 GW (Actual – 31 GW)
- Max hydro made available by 20:45 and ramped down
- Thermal and renewables ramped down (-7GW, -2GW)
- SCED was suspended at 18:00
- 200+ 400kV lines switched out
- Statcoms in voltage control mode, reactors switched in
- Frequency ranged from 49.7 to 50.25 Hz
  - Tx connection wind generation had high frequency trip out set to 50.2 Hz
  - Some indication limited tripping may have happened



POSOCO INITIAL REPORT

Data source: POSOCO

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Distribution System Topics

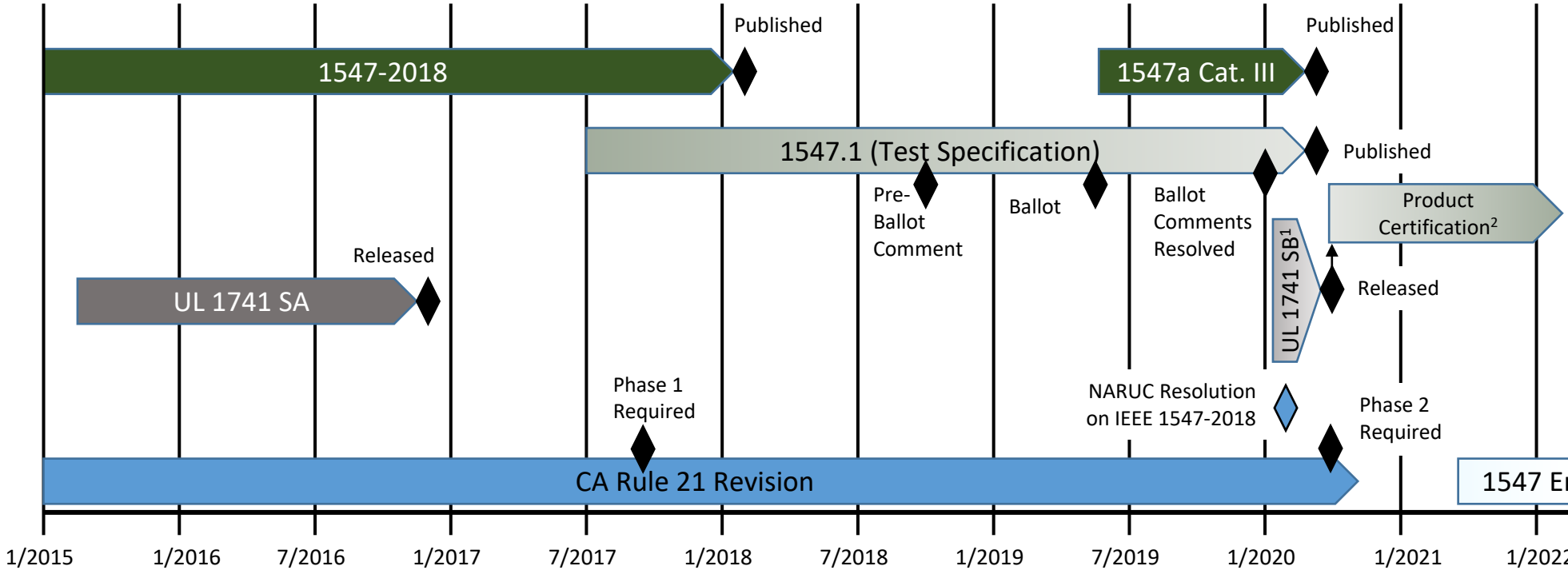
© 2020 Electric Power Research Institute, Inc. All rights reserved.

Outline of Topics

- IEEE 1547-2018 Review and Timeline
- EPRI DER Integration Engagement
- DER Autonomous Functions
- DER Control/Management (DERMS)
- Key EPRI DER Interconnection Research

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Timeline for Rollout of IEEE Std 1547™-2018 Compliant DER



Notes

[1] The new UL 1741 Supplement SB will directly refer to IEEE 1547.1-2020 and will be the only test procedure to certify IEEE 1547-2018 compliance. The existing Supplement SA will remain for the time being for those codes that continue to reference UL 1741 SA.

[2] Products to market not generally available until 18 months after release of IEEE 1547.1-2020 and UL 1741 SB.

Example Enforcement Dates

- MN: at "Commission Notice"
- MD: Jan 1, 2022

© 2020 EPRI

See also: https://site.ieee.org/sagroups-scc21/standards/1547rev/

Adoption of CA Rule 21 and Hawai'ian Rule 14H by inverter certification per UL 1741 SA.

Stopgap solution for **adoption of parts of IEEE Std 1547-2018** by inverter certification per UL 1741 SA.

Full adoption of IEEE Std 1547™-2018 by inverter certification per UL 1741 SB

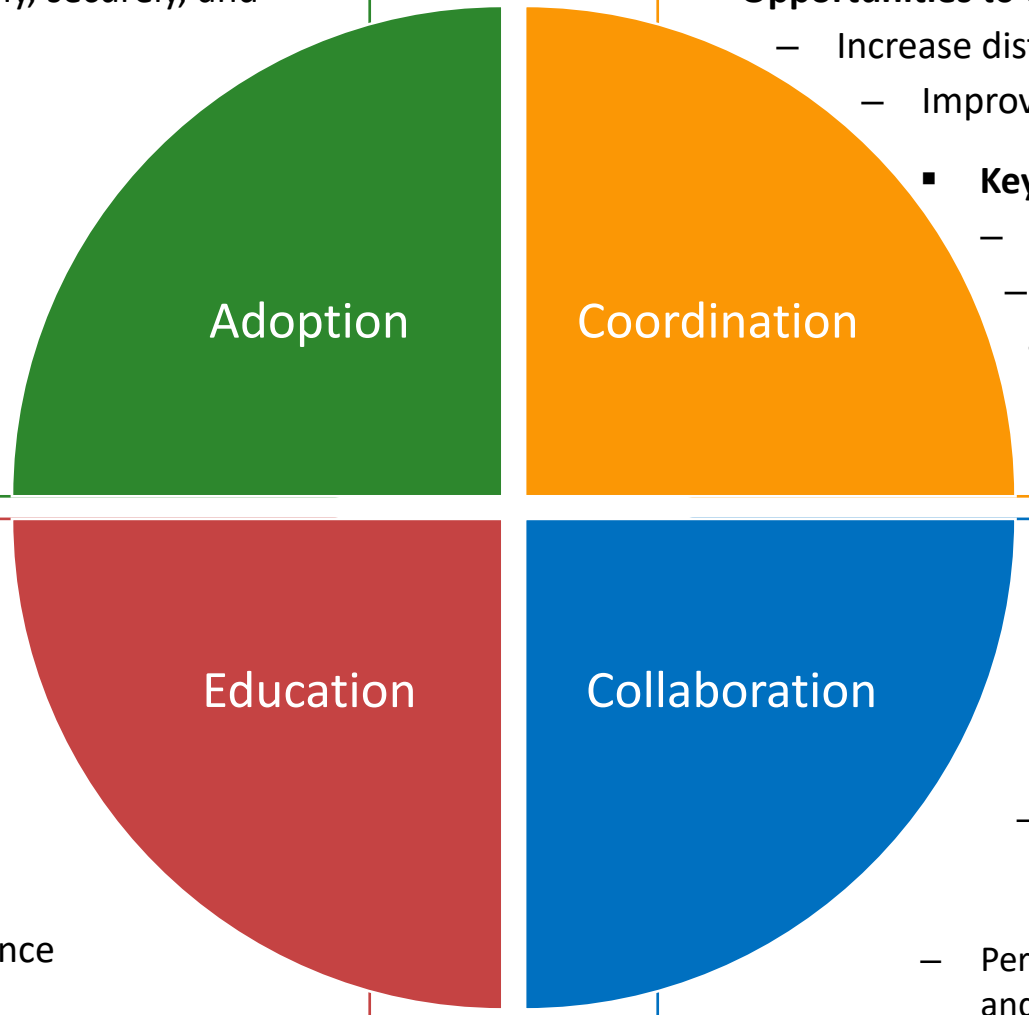
Question from **distribution** perspective:

Need to increase DER Integration?

Question from **transmission** perspective:

Need to address bulk system reliability?

EPRI DER Integration Engagement



- **Opportunities** to integrate DER reliably, securely, and efficiently into the grid
- **Key Considerations**
  - Consider adoption of standard at state-level
  - Specify "preferred" utility-required DER functional settings
  - Specify certification for DER equipment and potentially verification for DER facilities

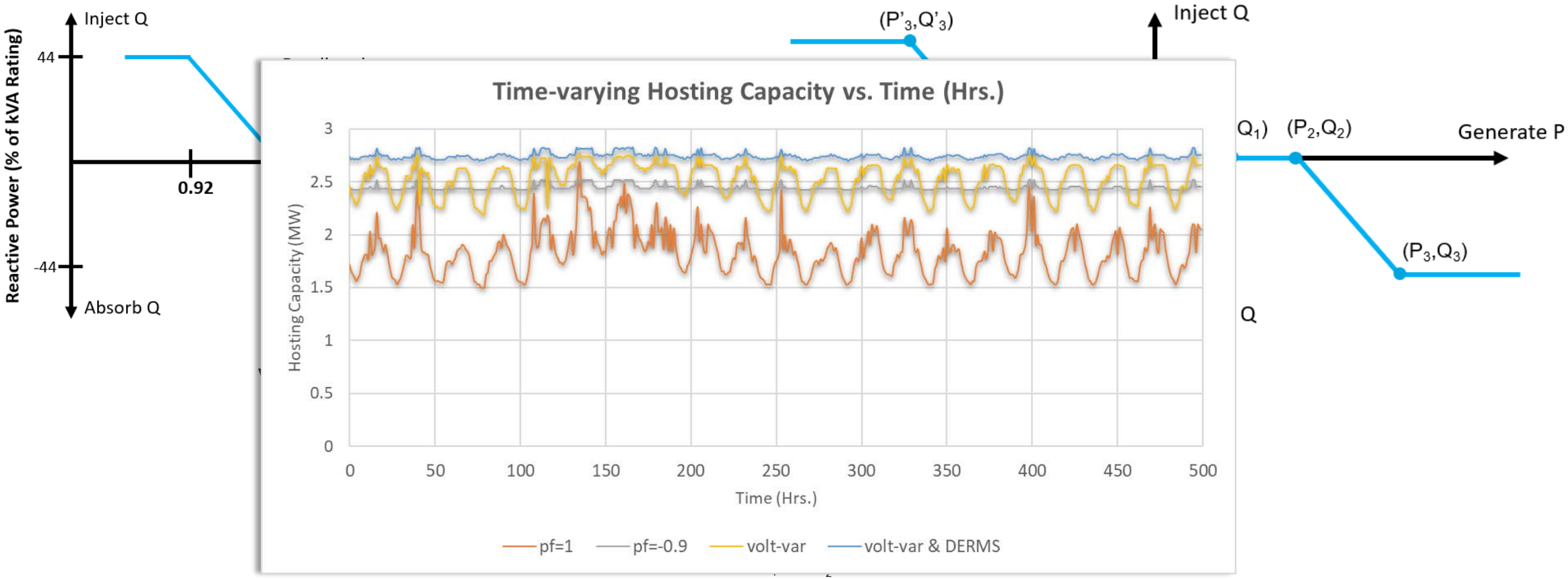
- **Opportunities** to utilize advanced DER capabilities
  - Increase distribution hosting capacity
  - Improve bulk system reliability
- **Key Considerations**
  - Functional settings
  - Performance categories
  - Communication interface
- **Coordinate across T&D**

- **Opportunities** to engage a broad set of stakeholders
- **Key Considerations**
  - Understand the key implications of the changes to the standard
  - Engage all parties in the education process
  - Learn how the standard may influence past regulatory decisions

- **Opportunities** to work collaboratively to solve issues
- **Key Considerations**
  - Engage state and federal agencies to advance understanding
  - Developers, utilities, and regulators collaborating to solve interconnection challenges
  - Perform research to understand best practices and develop policy objectives

© 2020 Electric Power Research Institute, Inc. All rights reserved.

What Are Advanced Autonomous DER Functions?

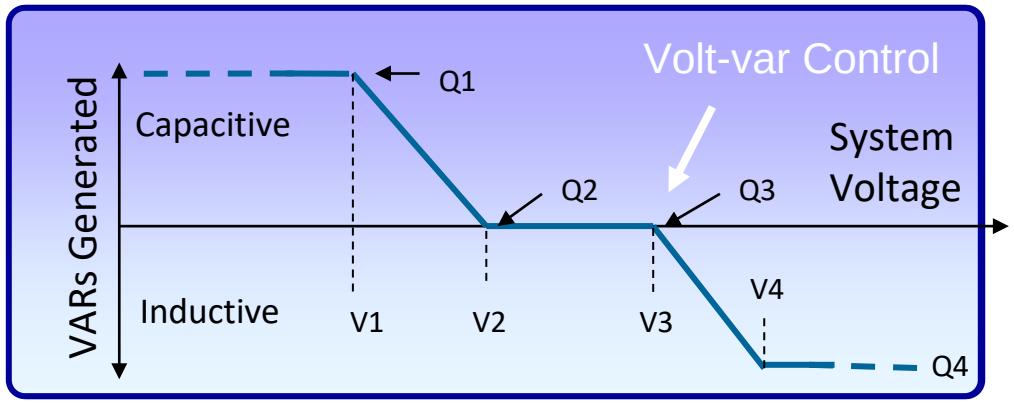


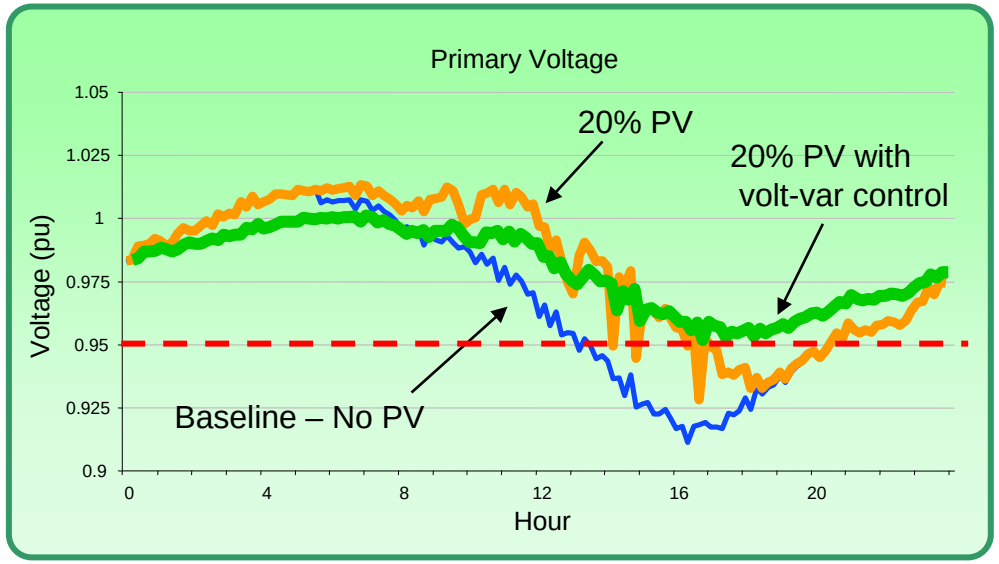
Volt-watt

A Potential Tool to Increase the Ability to Integrate DER while Managing Distribution System Constraints

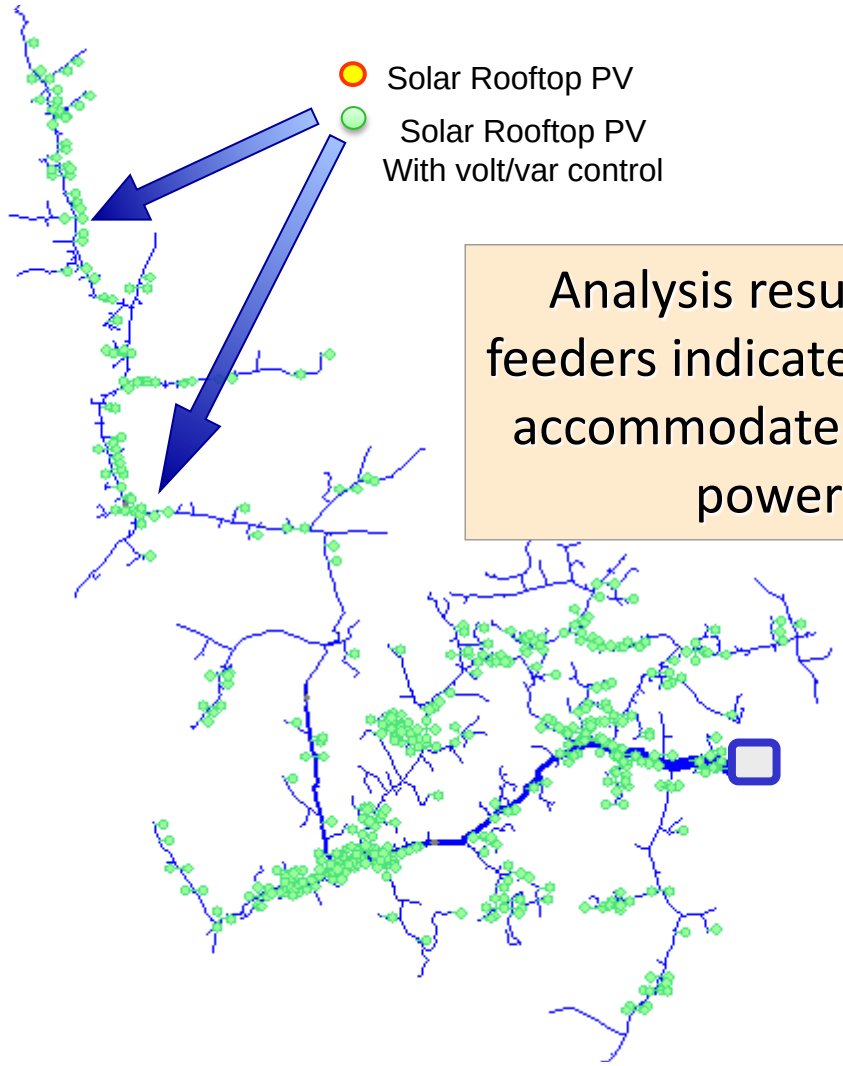
© 2020 Electric Power Research Institute, Inc. All rights reserved.

DER Reactive Power Support





24 Hour Simulation

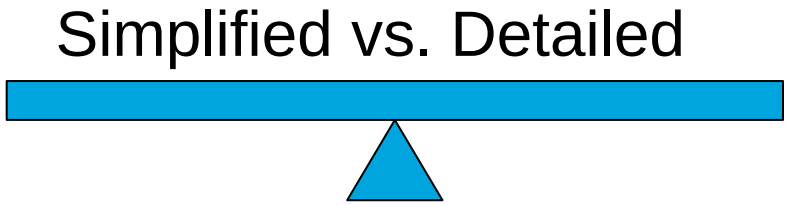


Analysis results from other feeders indicate more PV can be accommodated using reactive power control

© 2020 Electric Power Research Institute, Inc. All rights reserved.

DER Advanced Functions/Settings

- The Challenge
  - Already or potentially large volumes of requests
  - Requests for both small residential + large-scale
  - Cannot perform detailed study of every application… especially small residential
  - Limited field experience with latest functions/settings
- Key EPRI Research Objectives
  - Lead development of standards
  - Improve capability to integrate DER
  - Distillation of past research into guidelines
  - Develop methods for analysis



© 2020 Electric Power Research Institute, Inc. All rights reserved.

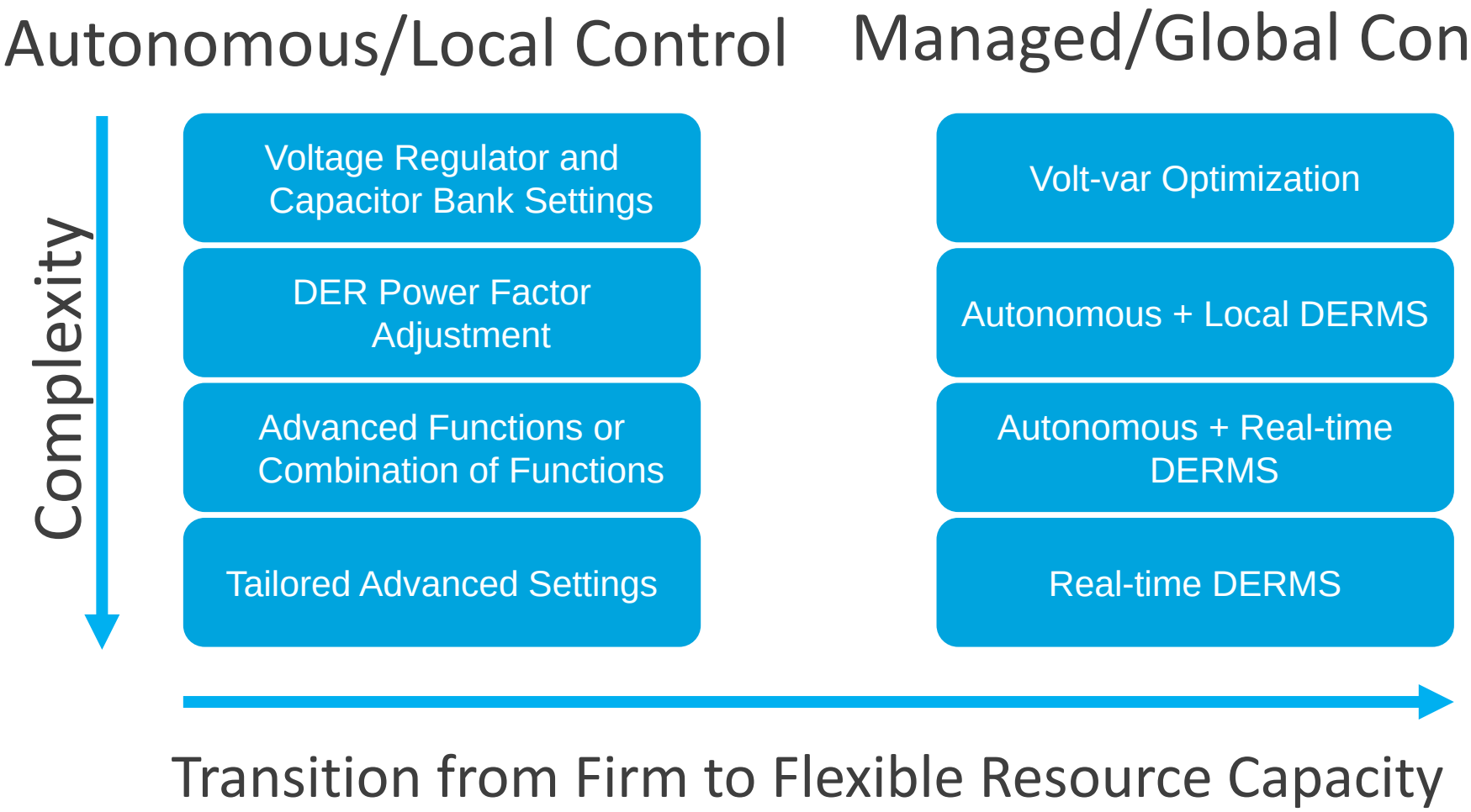
Advanced Function Actually Required in Field Today*

Utility/Region	Required Activated Function	Notes
Ameren, ComEd, MidAmerican	Volt-var (similar to CA Rule 21)…must be able to accept external commands	Associated with FEJA, up to 2MW projects initially
PG&E, SCE, SDG&E	CA Rule 21 Volt-var	Since July 2018, applies to all systems
Idaho Power	Tailored Volt-var	Applies to large, utility scale systems
Hawaiian Electric Company (HECO)	HI Rule 14 Volt-var	Since Jan. 2017, Volt-watt on selected systems
Germany DSOs	Volt-var, Q(P)	One DSO requires comms for >500kVA allowing settings adjustments
Endeavour Energy, Australia	Volt-var	Per AS/NZS 4777
NY Utilities	**Unity PF where possible, no advanced functions**	**Some demonstrations and considering in the future**

*This is not a comprehensive list and reflects data collection in progress

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Potential Control Solutions to Mitigate Voltage Constraints

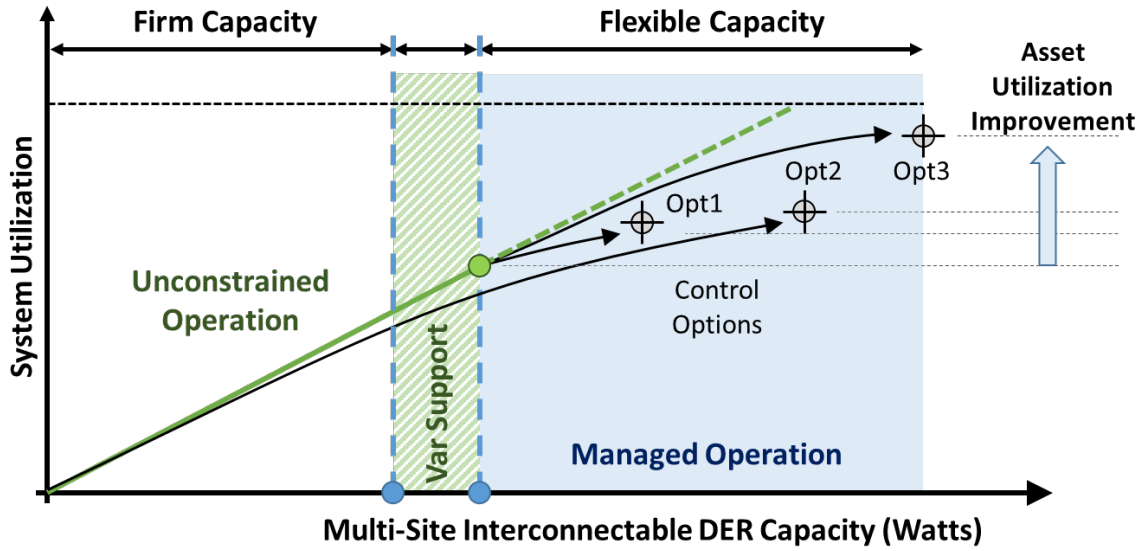


© 2020 Electric Power Research Institute, Inc. All rights reserved.

Maximizing DER Hosting and Grid Utilization through Flexible Interconnection Capacity Solutions (FICS)

Research Questions

- How does location affect flexibility?
- How to estimate nodal and zonal flexibility?



Scope/Approach

- Analyze many feeders and constraints
- Examine a broader set of load and generation forecasts
- Develop metrics to convey flexibility

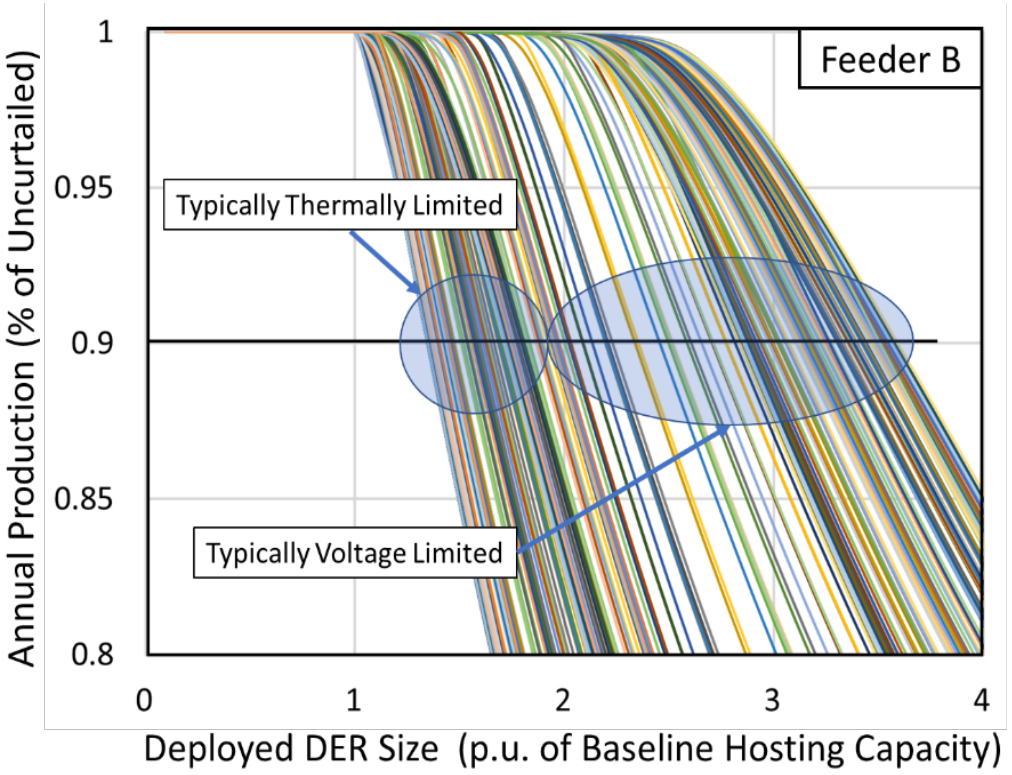
Expected Outcome

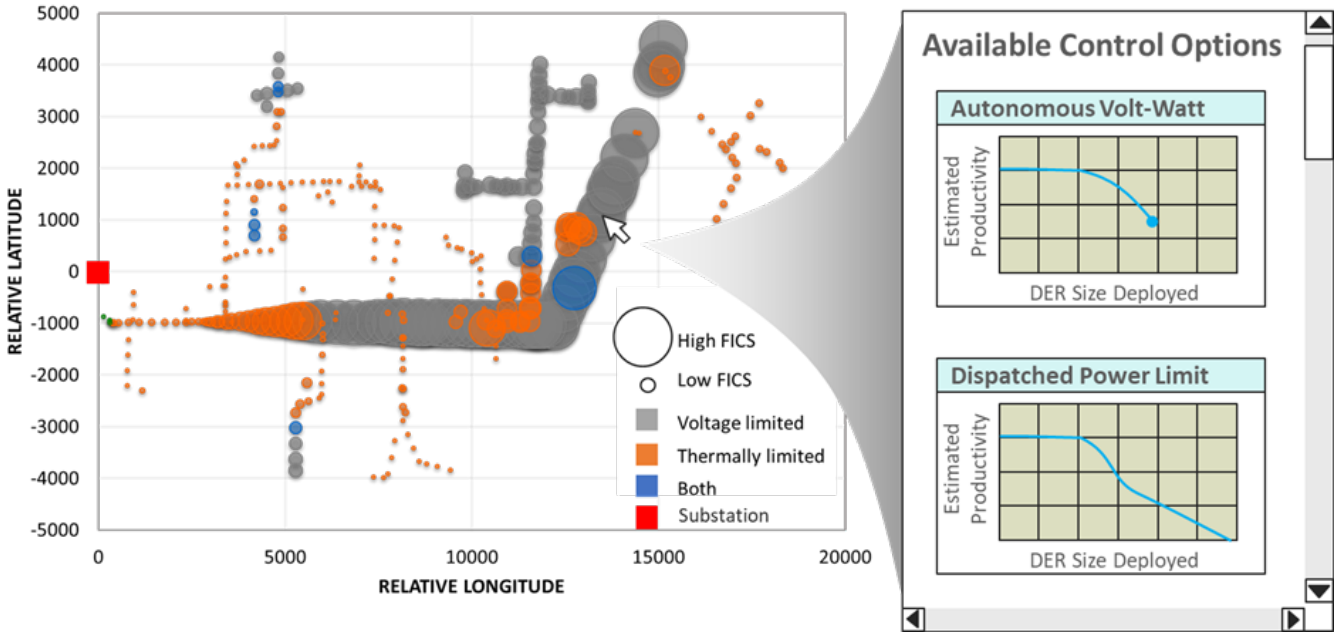
- Methodologies to quantify the impacts of Flexible Interconnection schemes
- Determine economic value

Flexible Interconnection Solutions Opportunity Guidance

© 2020 Electric Power Research Institute, Inc. All rights reserved.

FICS: Example Results





Widely Varying Flexibility Along a Feeder

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Meter Data Management System (MDMS)

Geographic Information System (GIS)

Customer Information System (CIS)

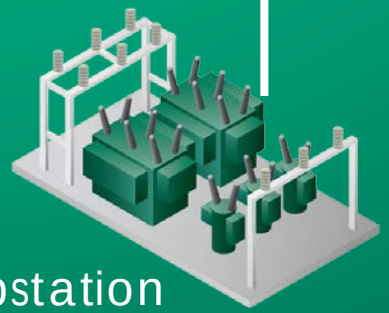
Enterprise Service Bus

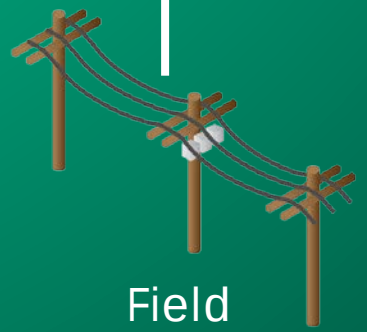
Distribution Management System (DMS)

DER Management System (DERMS)

?

Utility Network





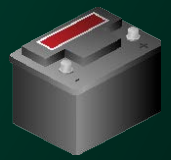
Substation Equipment

Field Devices

10's to 100's









Wind

Solar

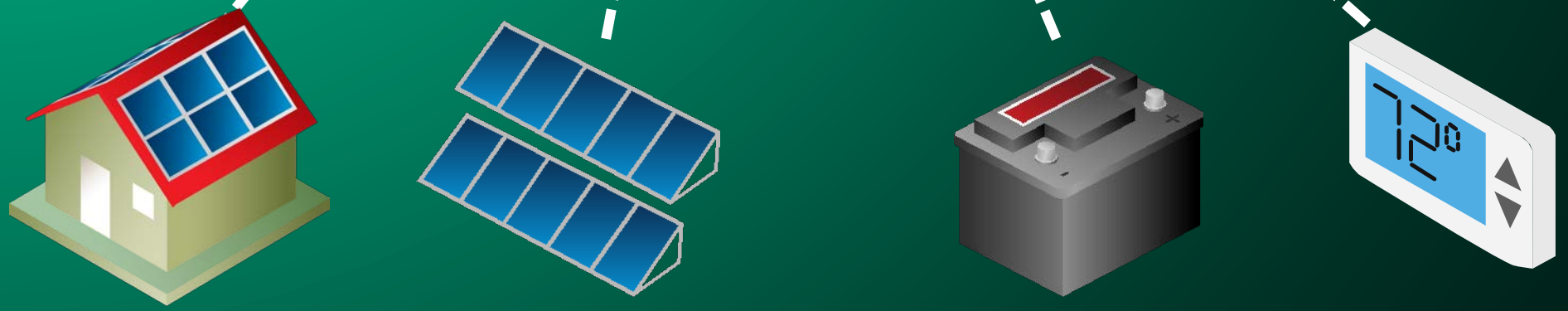
Storage

Demand Response

Thousands to Millions?

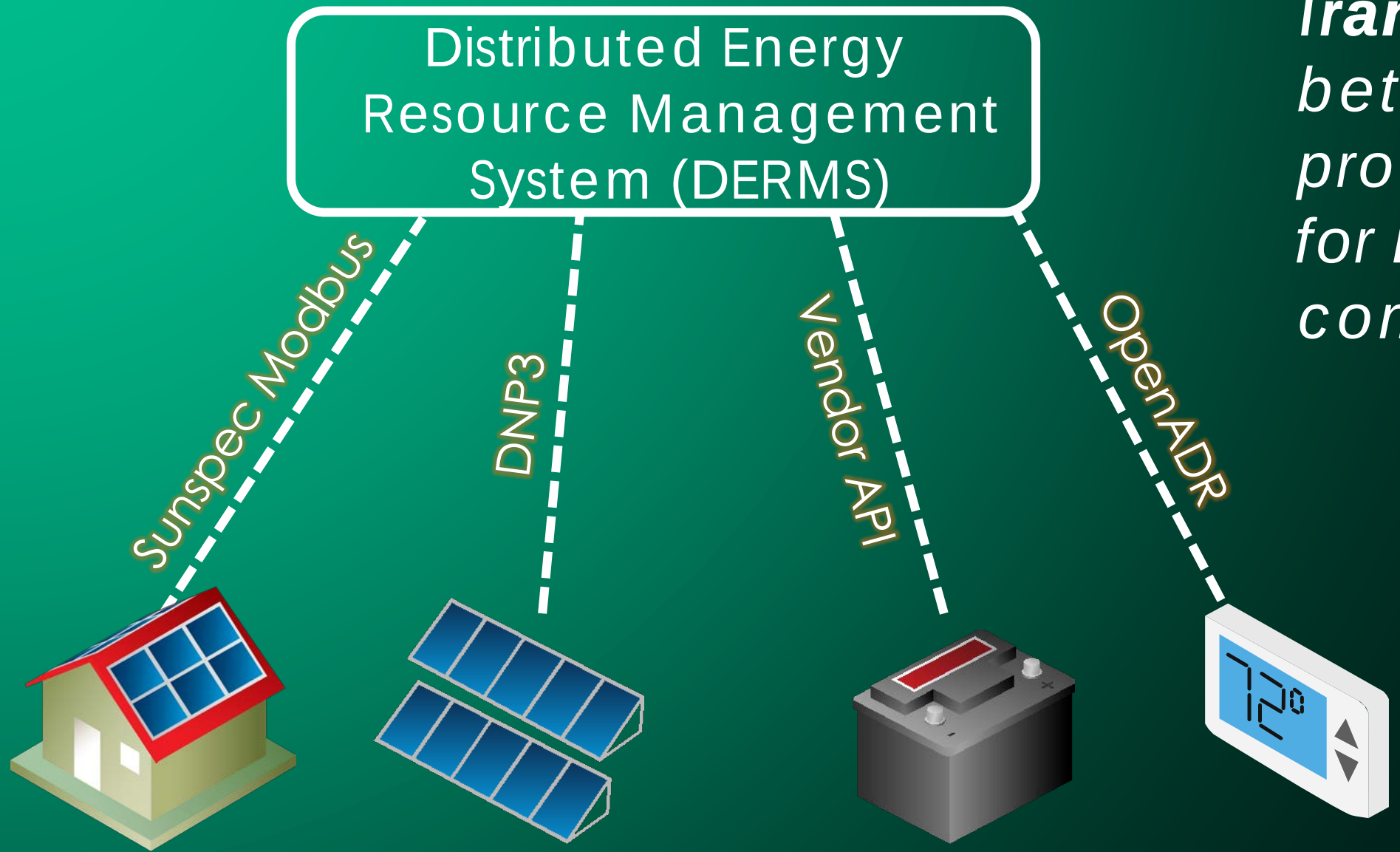
© 2020 Electric Power Research Institute, Inc. All rights reserved.

Distributed Energy Resource Management System (DERMS)



What exactly is the role of the DERMS?

© 2020 Electric Power Research Institute, Inc. All rights reserved.



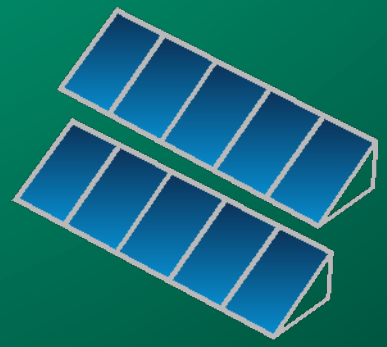
Translate *between various protocols used for DER communications*

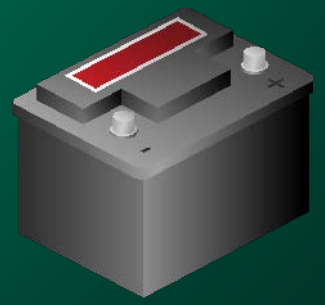
© 2020 Electric Power Research Institute, Inc. All rights reserved.

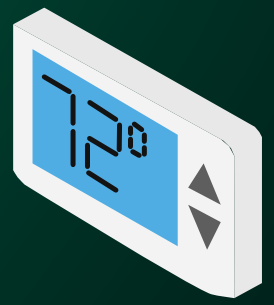
Distributed Energy Resource Management System (DERMS)

Aggregate up to millions of DER into combined, virtual resources



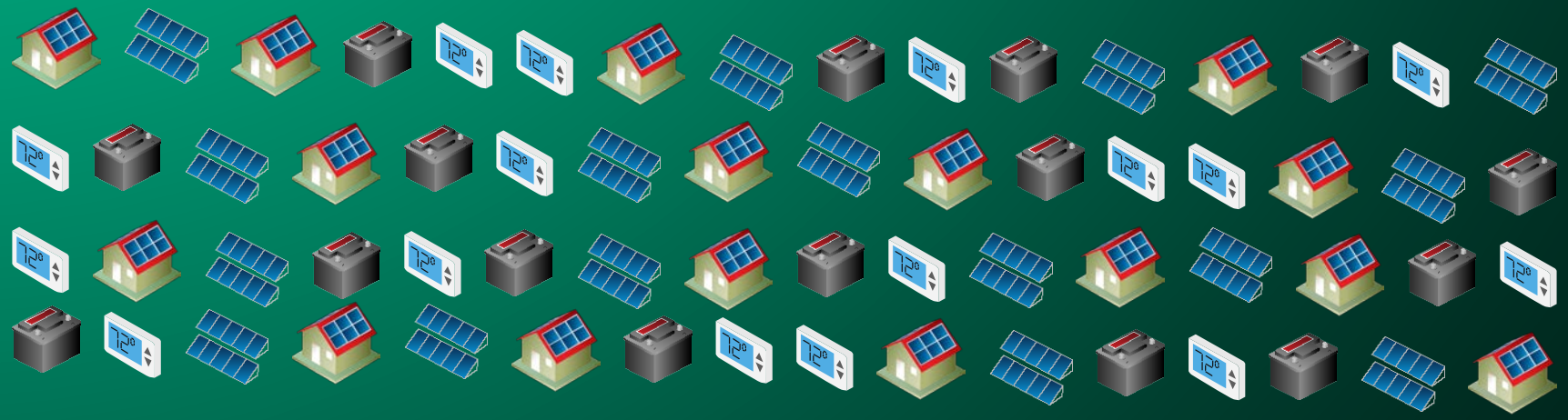






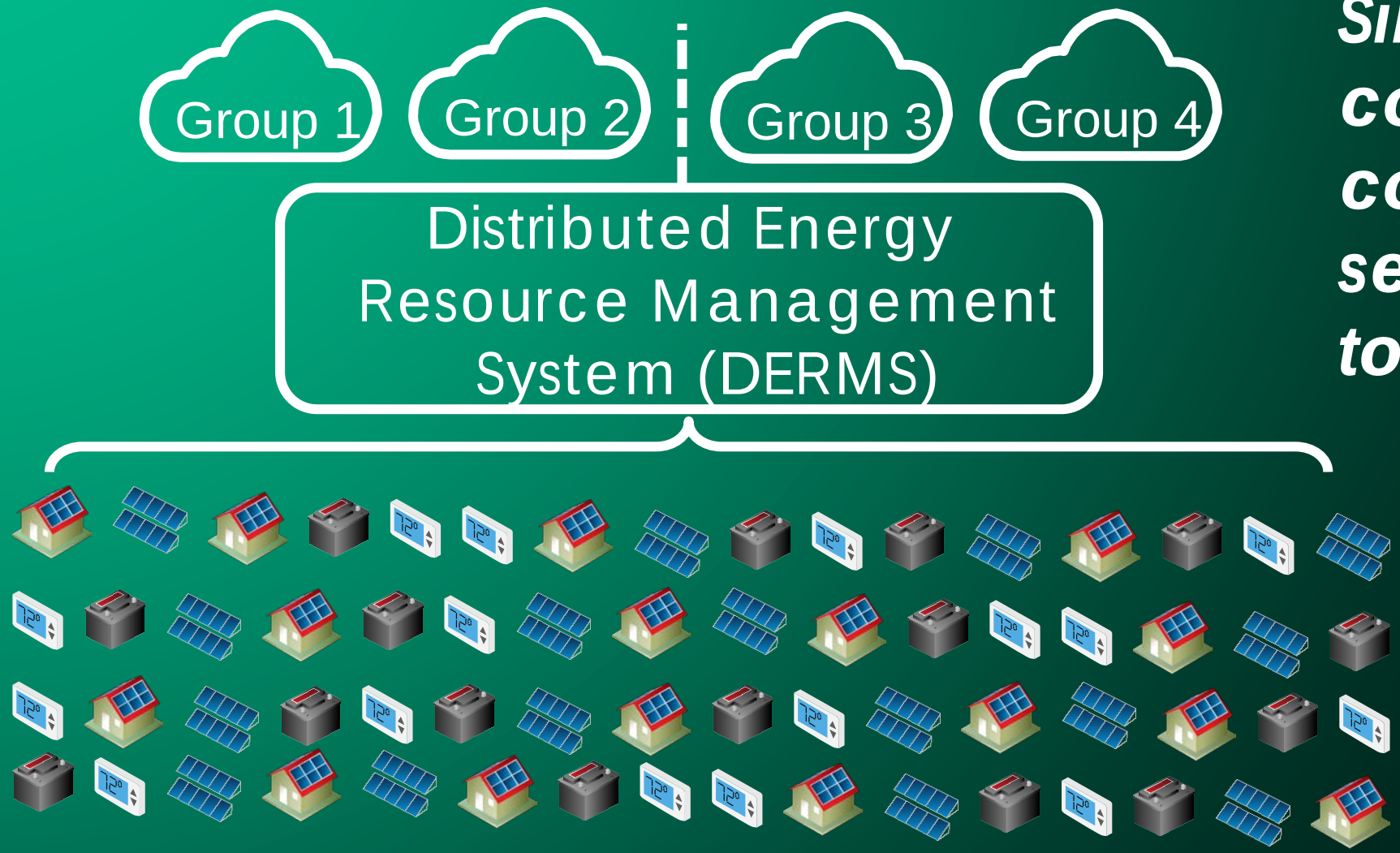
© 2020 Electric Power Research Institute, Inc. All rights reserved.

Distributed Energy Resource Management System (DERMS)



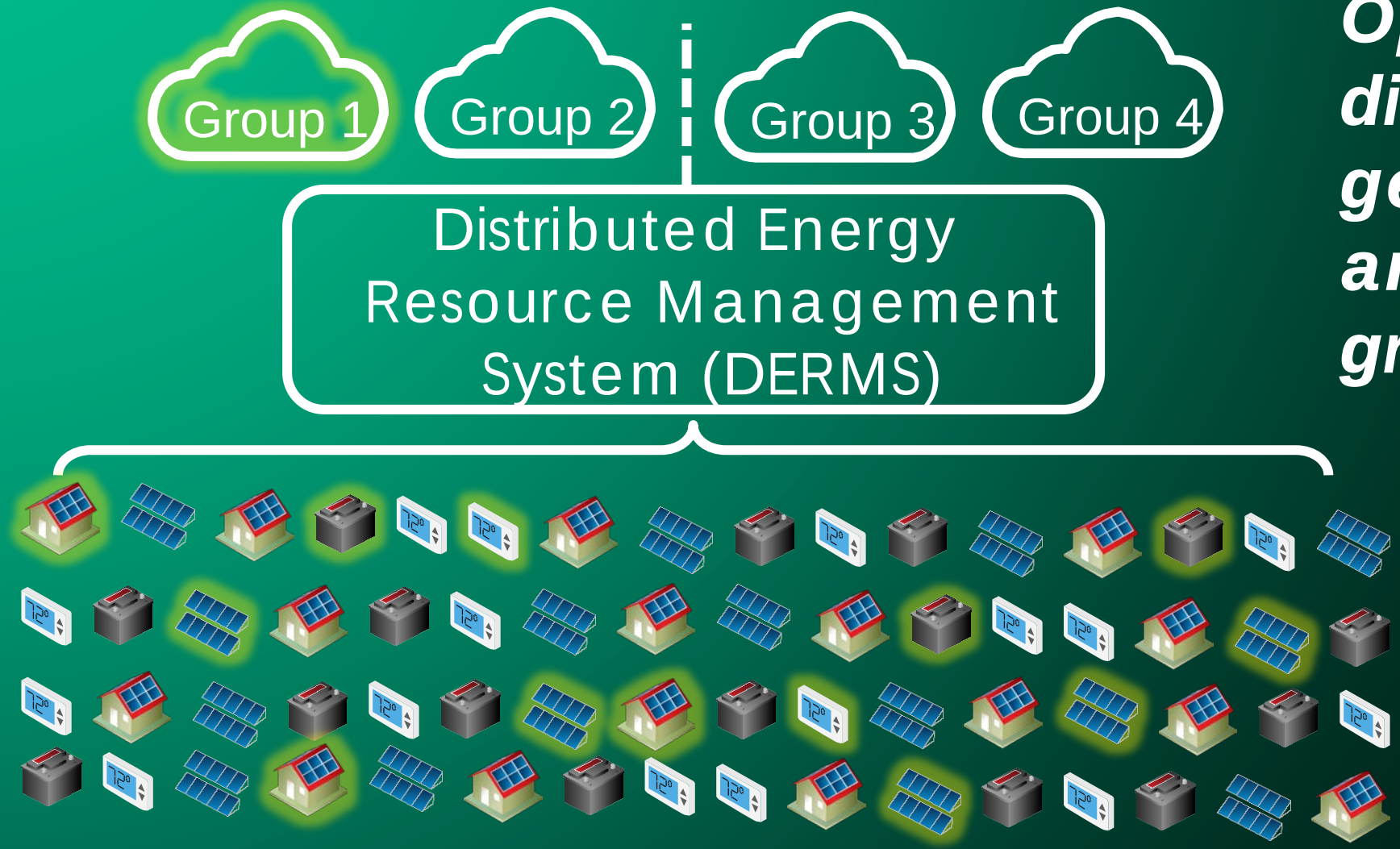
Aggregate up to millions of DER into combined, virtual resources

© 2020 Electric Power Research Institute, Inc. All rights reserved.



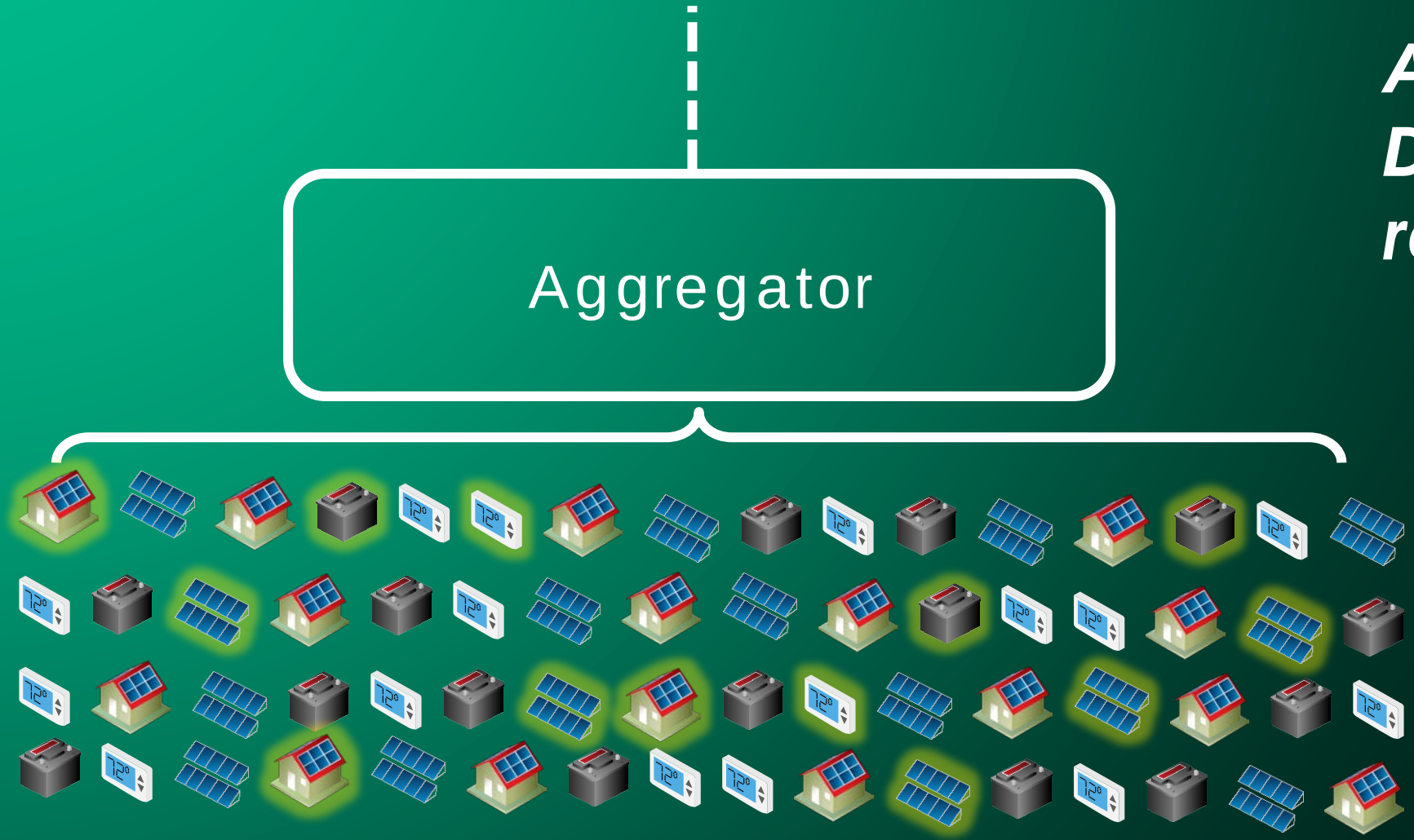
Simplify varied, complex DER commands into services useful to grid operators

© 2020 Electric Power Research Institute, Inc. All rights reserved.



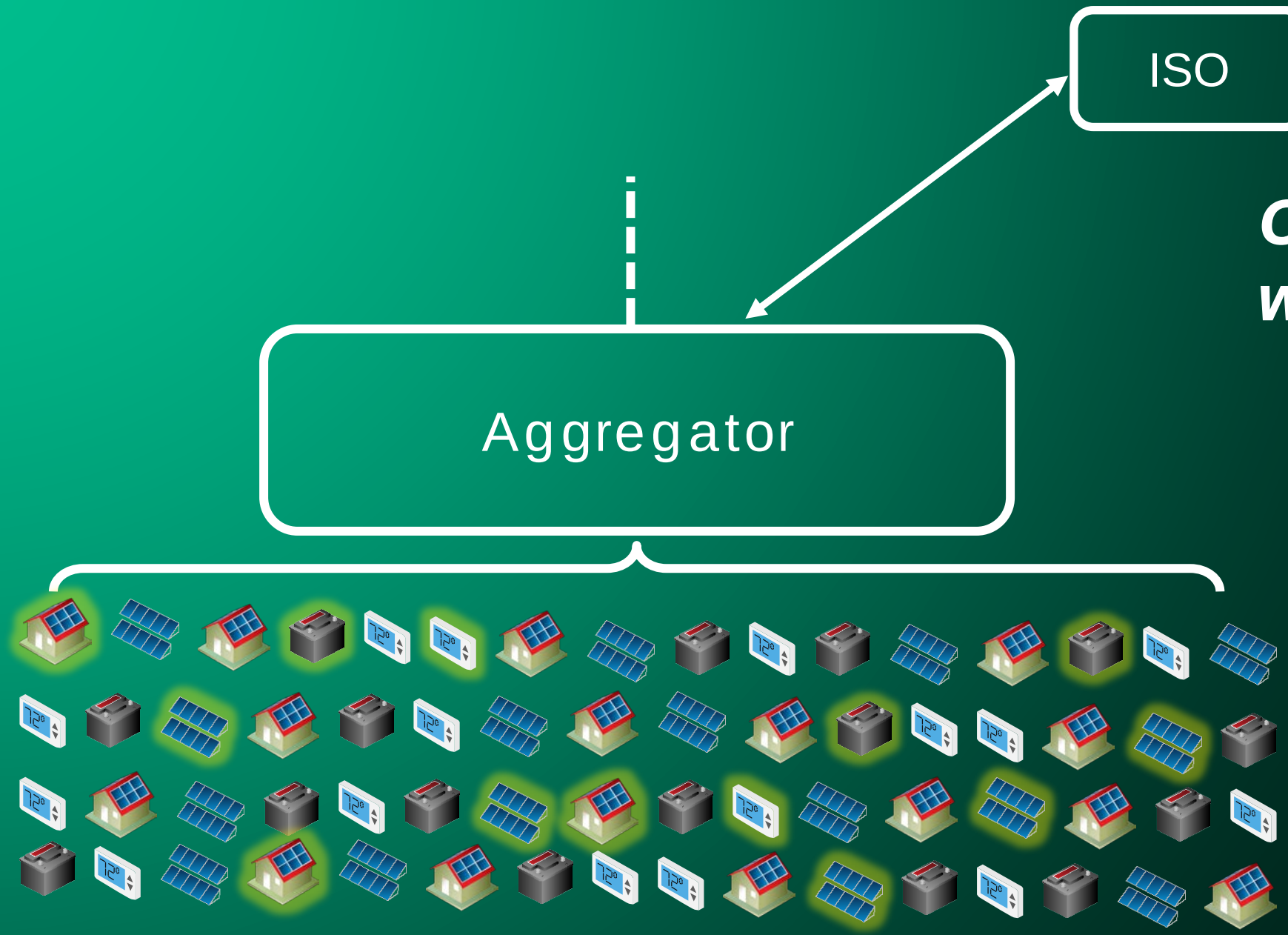
Optimize dispatch of general requests amongst grouped DER

© 2020 Electric Power Research Institute, Inc. All rights reserved.



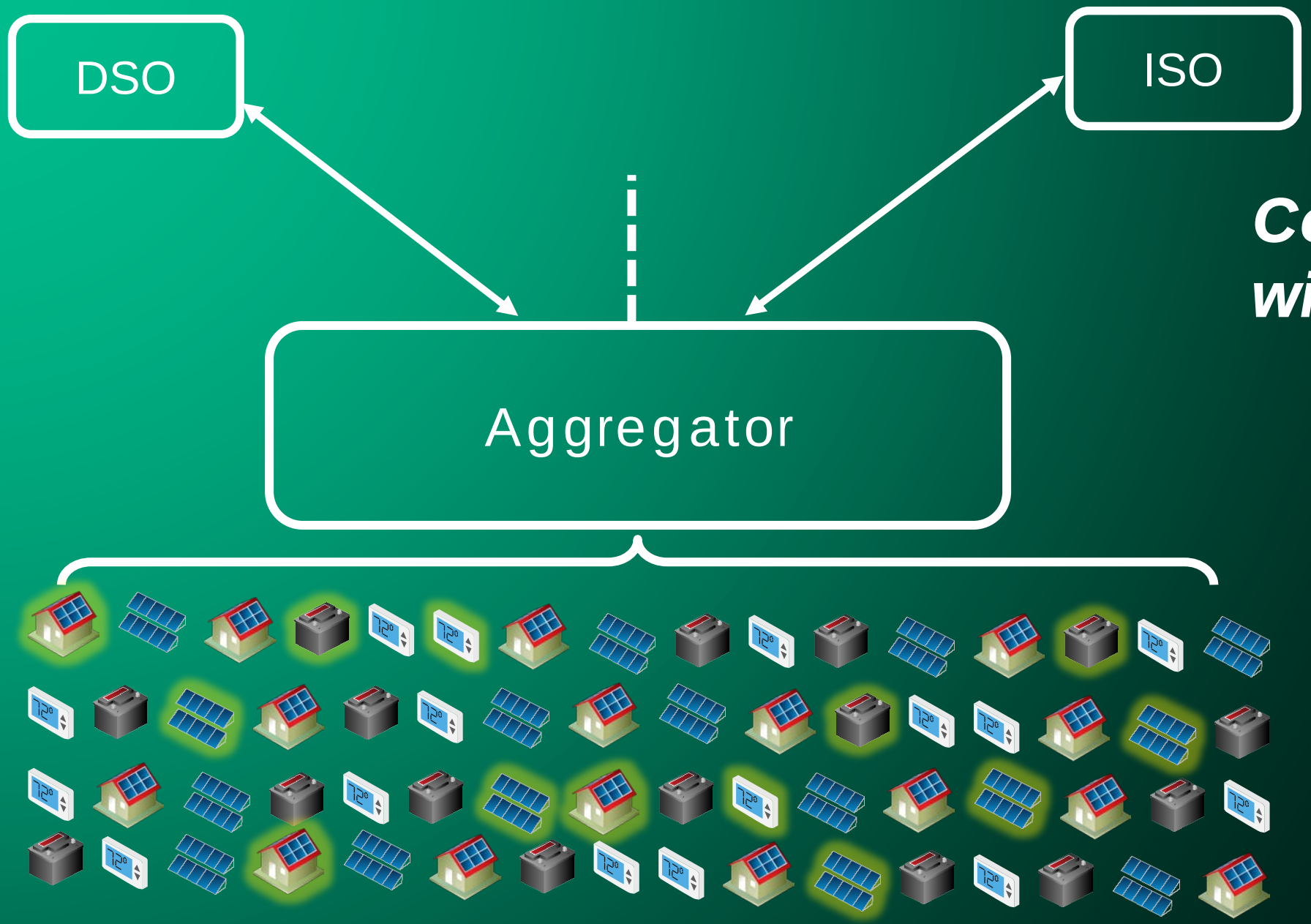
Aggregation of DER grouped resources

© 2020 Electric Power Research Institute, Inc. All rights reserved.



Coordination with ISO

© 2020 Electric Power Research Institute, Inc. All rights reserved.

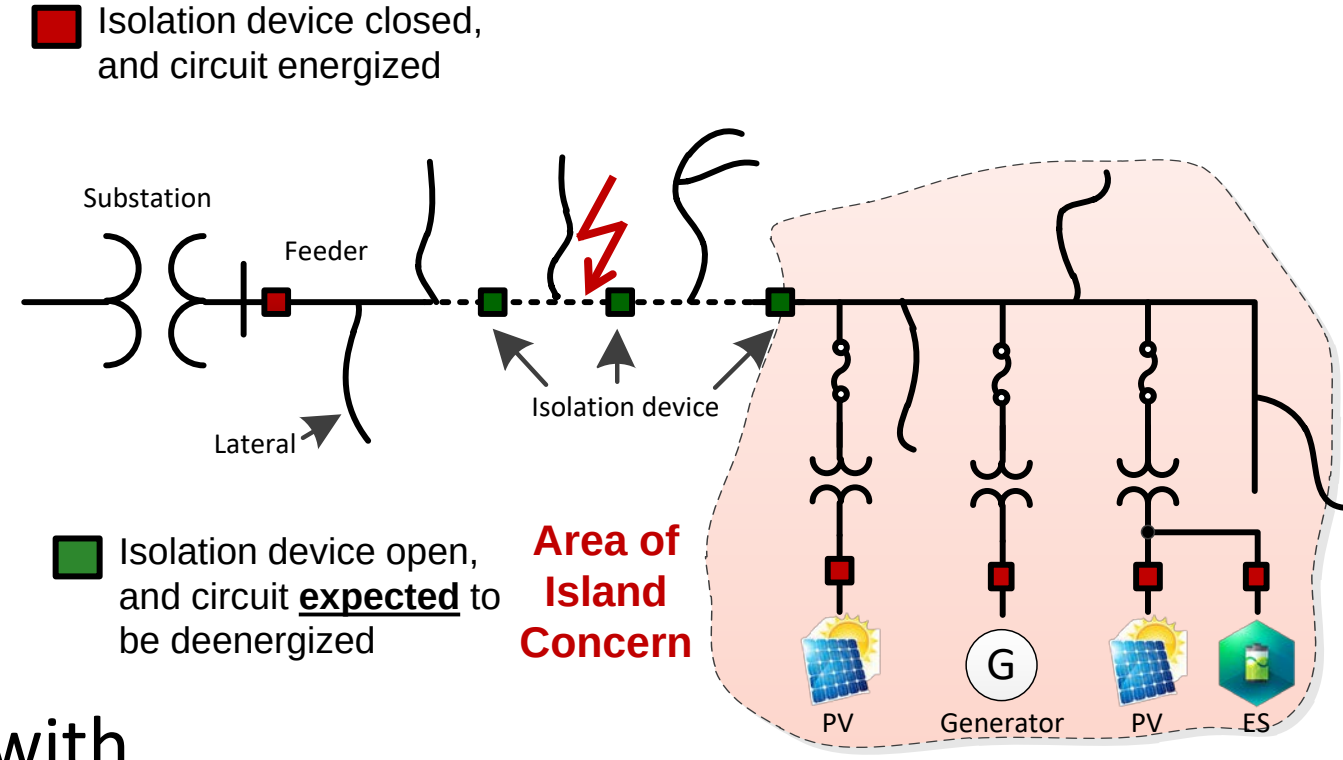


Coordination with ISO and DSO

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Summary of Key EPRI DER Interconnection Research

- Unintentional islanding detection
- Effective system grounding with inverter-interfaced DER
- Open-phase detection
- General protection coordination
- Direct transfer trip alternatives
- Field commissioning testing
- Voltage fluctuations/flicker
- Harmonic concerns
- Distribution automation impacts with DER
- Unintentional export control



© 2020 Electric Power Research Institute, Inc. All rights reserved.

Transmission System Topics



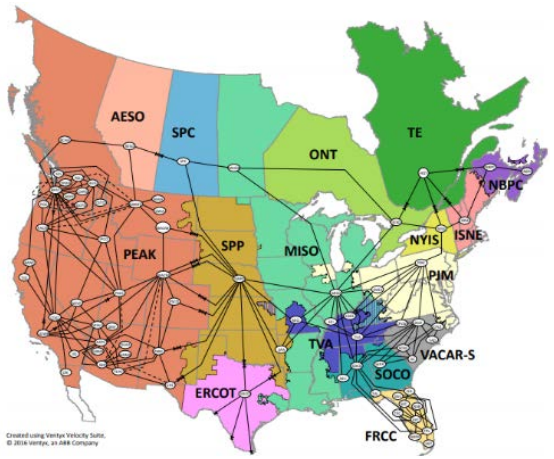
This presentation is, in part, supported by the U.S. Department of Energy, Solar Energy Technologies Office under Award Number DE-EE0009019 *Adaptive Protection and Validated MODels to Enable Deployment of High Penetrations of Solar PV (PV-MOD)*.

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Aggregate DER Impacts on Bulk Power System

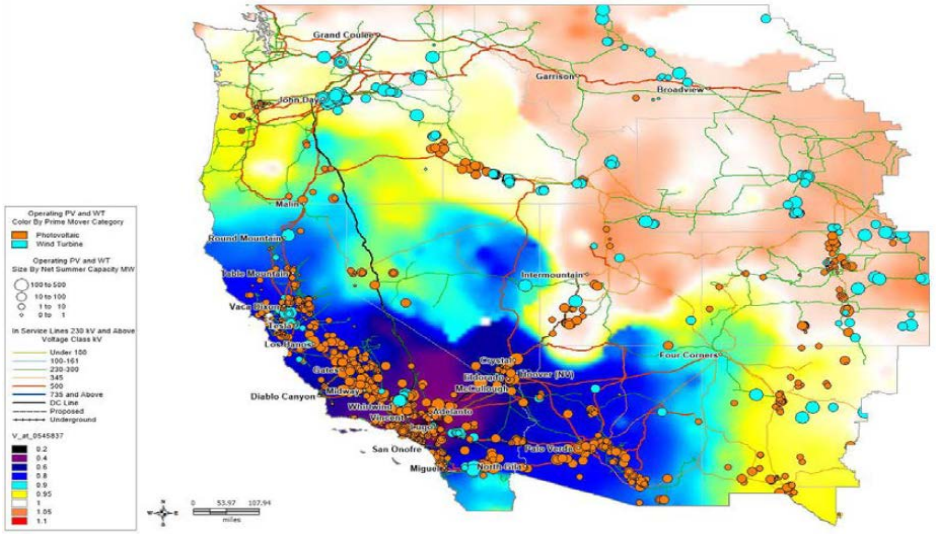
DER Frequency Tripping versus Ride-Through

- System frequency is defined by balance between load and generation
- Frequency is similar across entire interconnection
  - any DER exposed to large frequency deviations may trip simultaneously;
  - special concerns for system-split conditions
- Impact the same whether or not DER is on a high-penetration feeder
- NERC Reliability Coordinators
  - Colored entities in the map to the right



Source: NERC

DER Voltage Tripping versus Ride-Through

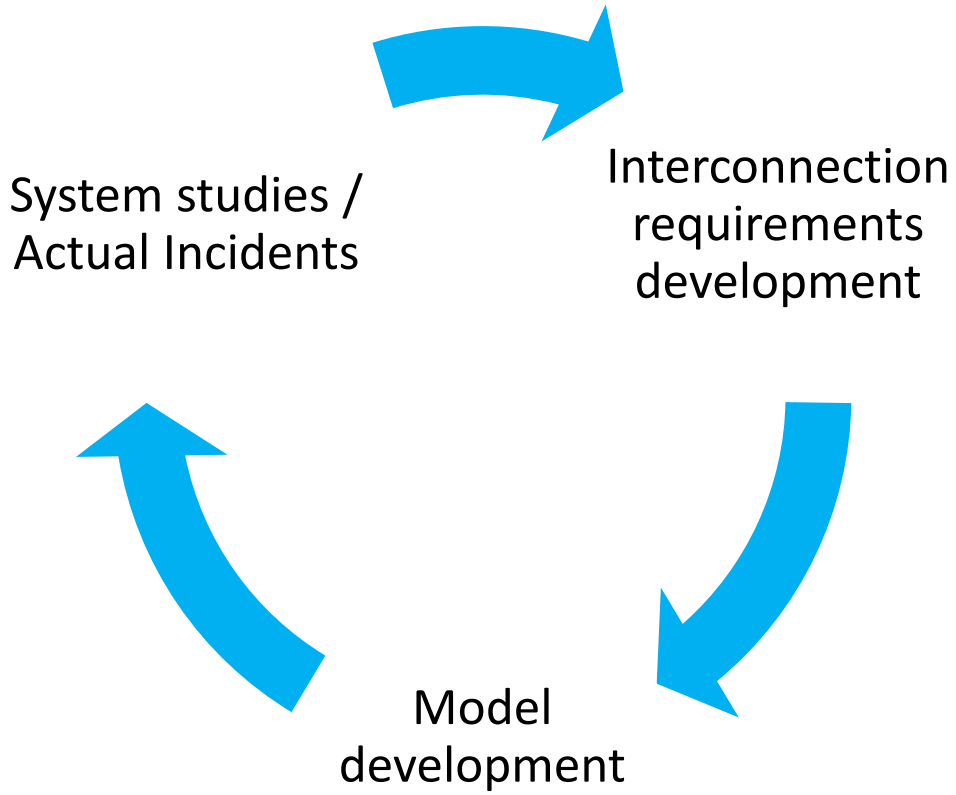


Source: SCE

- Transmission faults can depress distribution **voltage** over very large areas
- Sensitive voltage tripping (i.e., 1547-2003) can cause massive loss of DER generation
- Resulting BPS event may be greatly aggravated

© 2020 Electric Power Research Institute, Inc. All rights reserved.

EPRI Transmission Research Related to DER



IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces

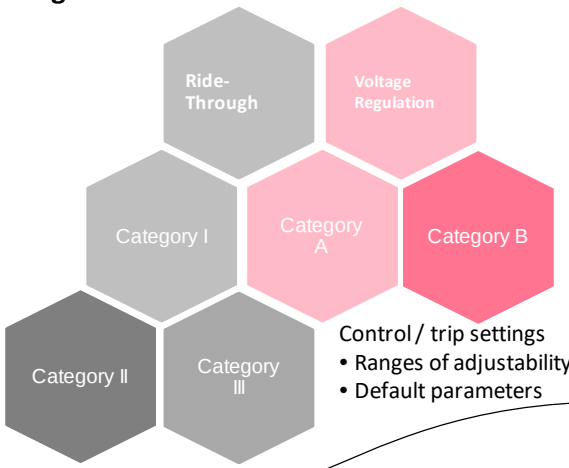
Available

IEEE Standards Coordinating Committee 21

Sponsored by the
IEEE Standards Coordinating Committee 21 on Fuel Cells, Pl
Generation, and Energy Storage

Also refer to supplemental project notice on "Navigating DER Interconnection Standards and Practices" (3002012048)

Normal and abnormal operating performance categories



Control / trip settings
- Ranges of adjustability
- Default parameters

Provide guidelines and tools to create a technical basis for assignment of `abnormal performance categories' specified by IEEE Std 1547-2018.

© 2020 Electric Power Research Institute, Inc. All rights reserved.

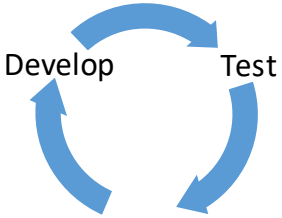
DOE PV-MOD: Project Overview

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

1 Resource Characterization

- Existing Models
- Lab Tests
- Field Data

2 Model Development



- Unit, Plant & Aggr. Feeder/BTM

3 Model Commercialization

- **Stability** (PSS/E, PSLF, …)
- **Protection** (CAPE, CYME, …)
- **EMT** (EMTDC, EMTP-RV, …)
- **QSTS** (CYME, Synergi,…)

4 Adaptive Protection Application

- Design
- HIL Testing

5 Demonstration

2020

- Field data collection
- Smaller kW inverter characterization (lab testing)
- Gap analysis of PV models (dynamic, short-circuit, EMT/HIL, PQ)
- Inverter models for quasi-static time series (QSTS)

2021

- Grid scale inverter characterization (NREL)
- Develop initial versions of refined or newly developed models
- Provide model specs to vendors
- Model validation using the newly developed models

2022

- Complete model validation
- Refine models based on validation
- Finalize specs for models & work with vendors

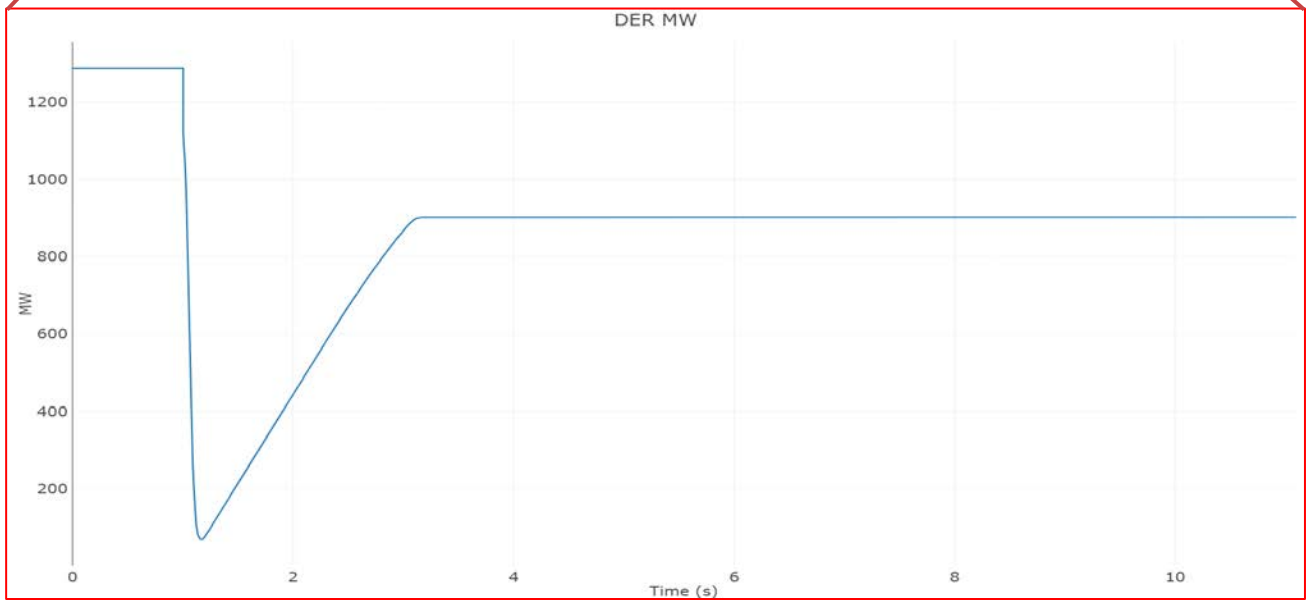
Validated; publicly available models for various types of studies, reports detailing the work, close collaboration with industry stakeholders (NERC, WECC, IEEE etc.)

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Actual DER Tripping Event Re-creation using Aggregate DER_A Model

- Comparing DER behavior to measured event
  - Disturbance occurred in off-peak season
    - Only summer peak case was available for simulations
  - Faulted line not identified
    - Picked lightly loaded line at identified substation
  - ~ 300 MW DER tripping in SCADA measurement
  - ~ 350 MW DER tripping in simulation
  - SCADA measurement covers several minutes, simulation covers seconds following fault
  - Using provided protection settings
    - vl0: 0.90 pu, vl1: 0.90 pu, tvl0: 0.167 s, tvl1: 0.167 s (10 cycles)





© 2020 Electric Power Research Institute, Inc. All rights reserved.

EPRI Member Case Study: Summary of load shed and generation shed

	P7 Contingency		Delayed Bus Contingency	
Scenario	MW / Mvar Load Shed	MW / Mvar Non - DER Generation Shed	MW / Mvar Load Shed	MW / Mvar Non – DER Generation Shed
Base Case	1858 / 513	0.0 / 0.0	1273 / 325	1858 / 485
1	2984 / 785	8672 / 1412	N/A	N/A
1a	2000 / 557	0.0 / 0.0	N/A	N/A
2	1992 / 555	0.0 / 0.0	N/A	N/A
3	1553 / 433	0.0 / 0.0	941 / 233	2182 / 605
4	1983 / 553	0.0 / 0.0	N/A	N/A
5	1553 / 433	0.0 / 0.0	941 / 233	2182 / 605
6	1553 / 433	0.0 / 0.0	941 / 233	2182 / 605
6a	1441 / 389	0.0 / 0.0	928 / 228	2182 / 605
7	1553 / 433	0.0 / 0.0	941 / 233	421 / 560

Impact of mom. cess.

Impact of DVS

Impact of Q priority

Impact of aggressive DVS

Impact of Cat III

Category III voltage ride-through capability beneficial for delayed-cleared faults.
Dynamic voltage support has limited impact.

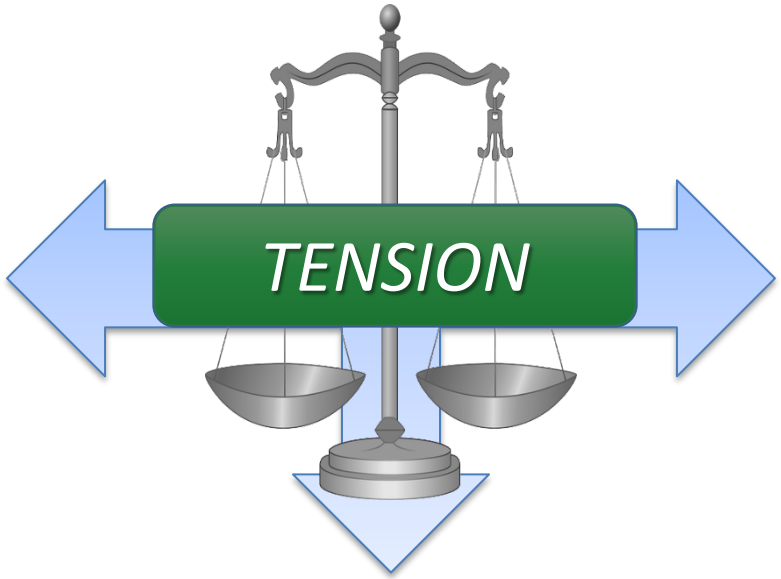
© 2020 Electric Power Research Institute, Inc. All rights reserved.

Balancing Bulk & Distribution Grid Needs

Public EPRI-U Webinars
3002014545
3002014546
3002014547

Distribution Grid Side

- Short trip times
- Ride-through *with momentary cessation*
- Voltage rise concerns
- Islanding concerns
- Protection coordination
- Safety of line workers



Bulk System Side

- Long trip times
- Ride-through *without* momentary cessation
- Reactive power support
- Frequency support

Increasing need for T&D Coordination

© 2020 Electric Power Research Institute, Inc. All rights reserved.

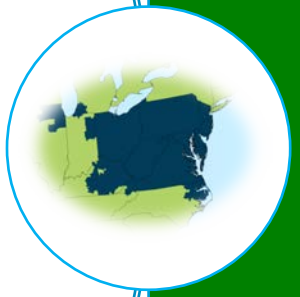
RTOs/ISOs Guidelines for IEEE Std 1547™-2018 Adoption



ISO New England

June 1, 2018

- Coordination between ISO-NE and the MA's utilities in the Massachusetts Technical Standards Review Group
- Reference to UL 1741 SA as a stopgap to verify DER ride-through capability in the interim
  - Harmonization of voltage & frequency trip settings with IEEE Std 1547-2018 ranges of allowable settings (Link)



PJM Interconnection

Jan 1, 2022

- Initiation of formal stakeholder proceedings in 2019
- Published PJM *Guideline for Ride Through Performance of Distribution-Connected Generators* for voluntary DER ride-through in Oct 2019 (PJM Website)
- Established minimum Ride-through requirements and trip time settings



Midcontinent Independent System Operator (MISO)

date not specified

- MN PUC requested stakeholder process, see MISO's IEEE 1547 website
- Published the MISO Guideline for IEEE Std 1547-2018 Implementation (Link)
- Established the preferred regional Ride-through capabilities and trip time settings

See also NERC's Reliability Guideline
Bulk Power System Reliability Perspectives on the Adoption of IEEE 1547-2018 (March 2020)

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Common Performance Category / Capability Assignments

Normal Performance Categories

Power Conversion	Prime Mover / Energy Source	Category
Inverter	Solar PV, Battery Energy Storage	Category B
	Wind	Category B
	Hydrogen Fuel Cell	Mutual Agreement
Synchronous generator	Bio-/landfill gas, fossil fuel, hydro, combined heat & power	Category A
Induction generator	Hydro	Mutual Agreement

Not in scope of NPCC guidance?

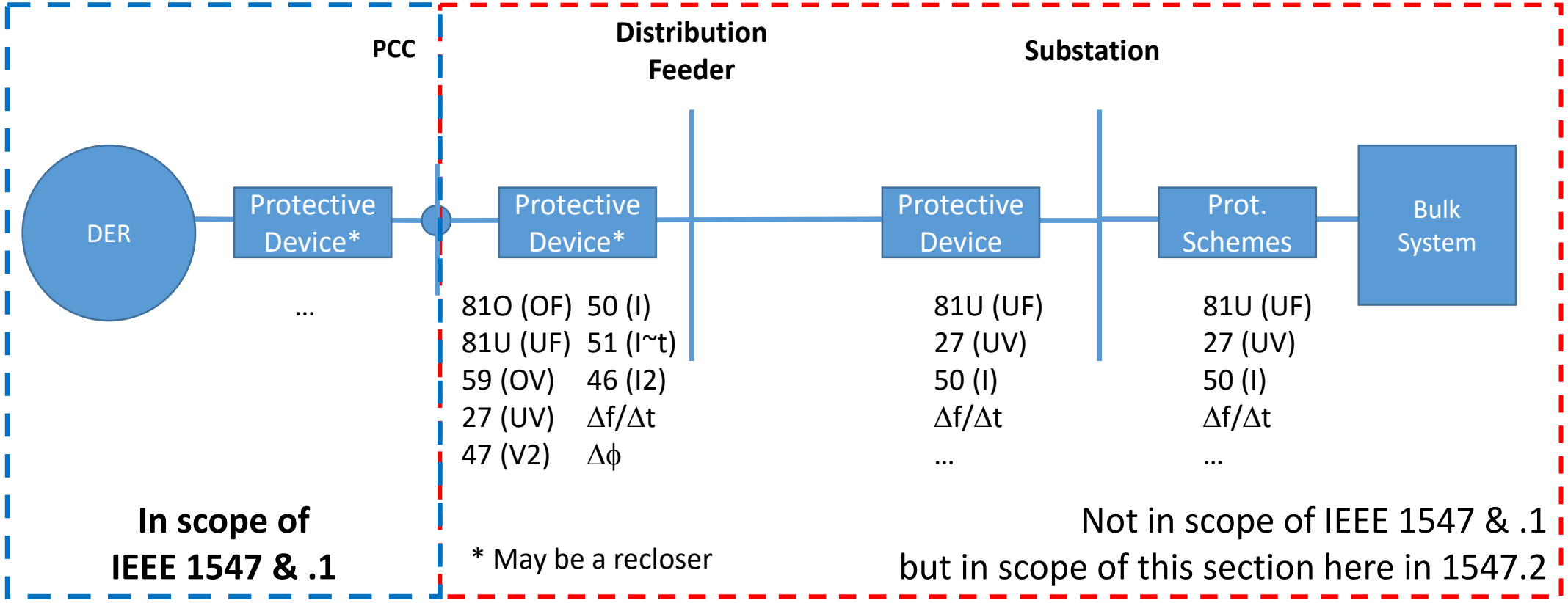
Abnormal Performance Categories

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

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Coordination of Distribution Protection Practices with DER Ride-Through



© 2020 Electric Power Research Institute, Inc. All rights reserved.

NPCC Specific Discussion

- Value Add of NPCC Guideline over NERC Reliability Guideline *Bulk Power System Reliability Perspectives on the Adoption of IEEE 1547-2018*?
  - *Abnormal performance category assignment*
  - *Functional settings impacting BPS (trip, frequency droop, etc.)*

- Work with distribution utilities regarding feeder & substation protection DER to coordinate with ride-through?

- Other Topics
  - Value of DER steady-state voltage/reactive power control?
  - Potential benefits & challenges of DER fault-related dynamic voltage support?

NPCC Reliability Guideline Could Provide Guidance to ISOs/RTOs and Distribution Providers

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Together…Shaping the Future of Electricity

Devin Van Zandt
+1 518.281.4341
dvanzandt@epri.com

Jens Boemer
+1 206.471.1180
jboemer@epri.com

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Backup

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Adaptive Protection and Validated MODels to Enable Deployment of High Penetrations of Solar PV (PV-MOD) / PRINCIPAL INVESTIGATOR: DR. JENS BOEMER (EPRI)

2064-1764

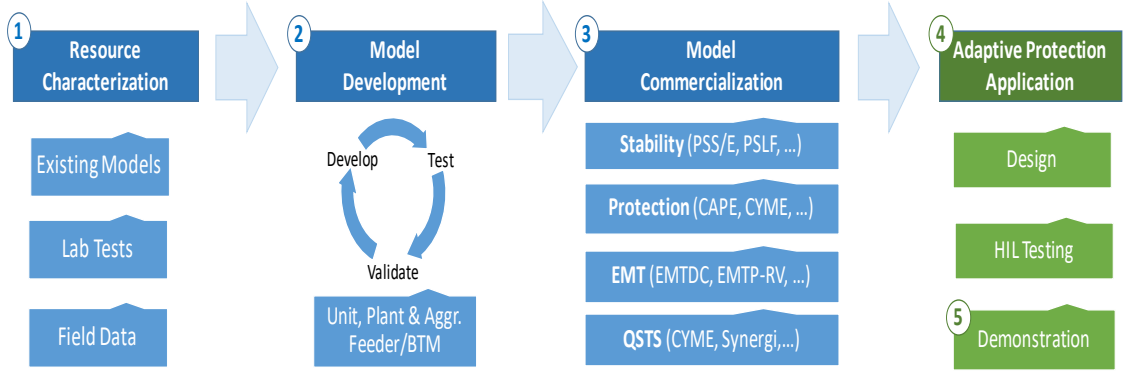
Project Objectives

Enabling deployment of higher levels of Solar PV by providing utilities, developers, and vendors with ***high-fidelity, validated*** unit and facility ***models*** *and* ***demonstrated adaptive protection schemes*** that represent and use advanced PV capabilities. ***Transformation*** of dynamic modeling approaches used in industry for planning and protection models of Solar PV by ***bridging the gap*** between model development and application-ready tools to ***ensure successful adoption***.

Technical Approach

Develop and ***validate*** high-fidelity ***models*** of solar PV facilities at ***all levels*** of the power system across ***all operational reliability time frames*** and ***integrate*** the validated models ***into commercial software tools and HIL platforms***[1] used by power system engineers to ***plan***, ***operate***, and ***protect*** transmission and distribution (T&D) systems by using EPRI's existing vendor engagement processes.

[1] Siemens PTI PSS®E, GE PSLF™, PowerWorld, DSATools TSAT, EMTP-RV, PSCAD EMTDC, DIgSILENT PowerFactory, RTDS, Opal-RT, Typhoon, Aspen OneLiner, Siemens PSS®CAPE, CYME, Synergi, and OpenDSS



Project Team

• **Lead:** EPRI • **Nat. Labs (sub):** NREL, ORNL • **Other**: Army Corps of Eng. (host site), PEACE (contractor) • **Utilities (host sites):** ConEdison, PPL • **Vendors:** FirstSolar, ASPEN (Oneliner), Siemens (CAPE), EATON (Cyme), ABB • **Utilities (support):** NERC, WECC, APS, Duke, NGrid, SoCo

Budget

Federal funds: $4.1M Cost-share: $1.5M (~27%) Total: $5.6M

Anticipated Outcomes

Year 1:	Inverter Characterization, Gap Analysis of PV Models, Initial Model Dev. & Validation, Gap Analysis and Adaptive Protection Scheme Design
Year 2:	PV Model Dev. & Refinement, Vendor Engagement, Validation, Modeling & HIL Testing of Adaptive Protection Schemes
Year 3:	PV Model Validation, & Vendor Engagement, Adaptive Protection Field Demos

	Project Tasks Timetable	BP1				BP2				BP3			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
1	Project Management, Vendor Engagement & Tech Transfer												
2	Field Data Collection												
3	Inverter Characterization												
4	PV Model Development, Refinement & Vendor Engagement												
5	Industry Assessment & Adaptive Prototype												
6	Inverter Characterization												
7	PV Model Development, Refinement & Vendor Engagement												
8	Model Validation												
9	Adaptive Simulations and HIL Tests												
10	Model Validation												
11	Field Demos and Industry Guide												
12	Project Report												

Transformative Modeling and Adaptive Protection Enabling Grid-Ready Applications

© 2020 Electric Power Research Institute, Inc. All rights reserved.

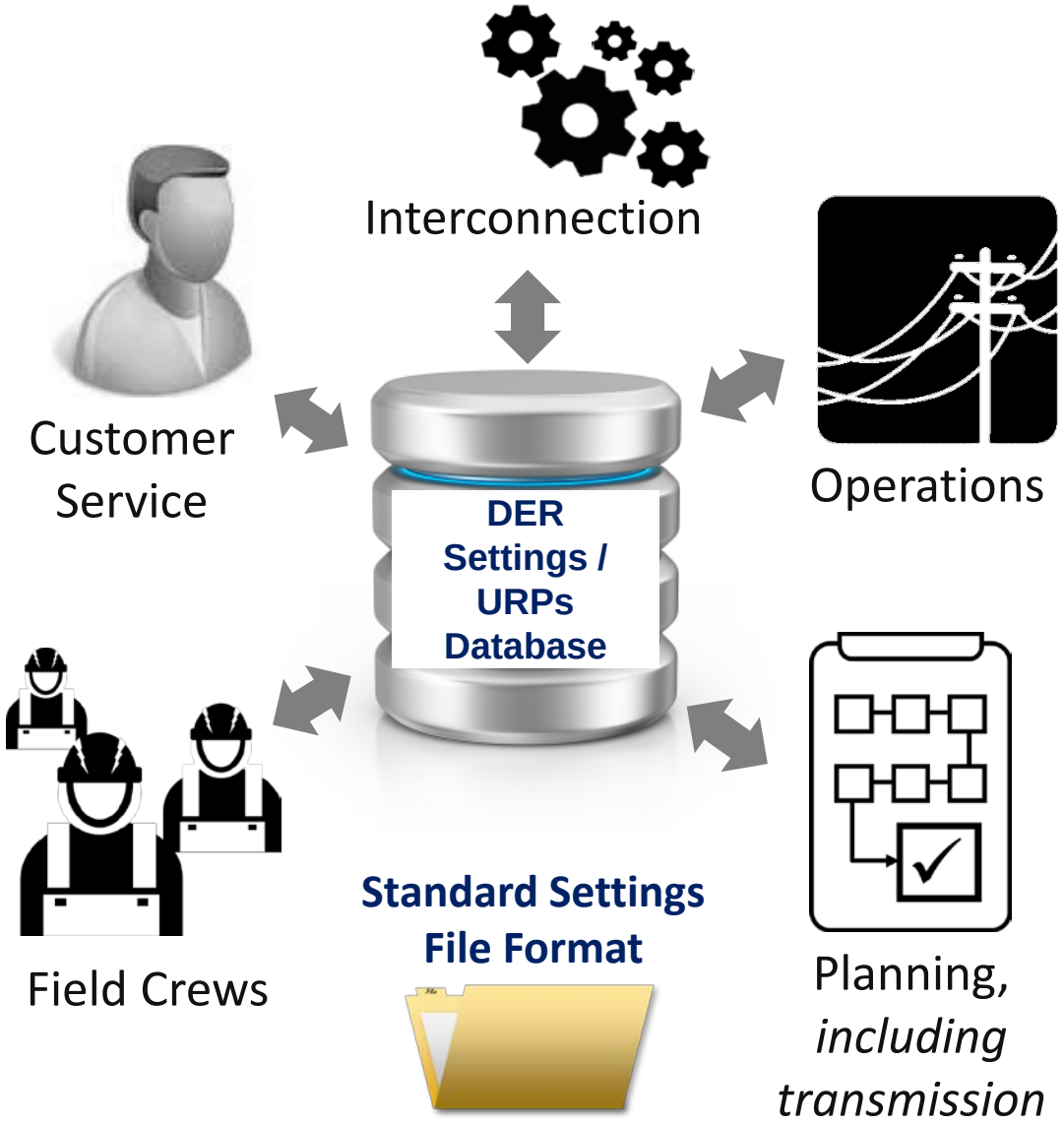
Dynamic Voltage Support is Only an Optional Requirement in IEEE 1547-2018

Function Set	Advanced Functions Capability	IEEE 1547-2003	IEEE 1547a-2014	IEEE 1547-2018	Rule 21 (Phases)	Rule 14H & UL SRDv1.1
All	Adjustability in Ranges of Allowable Settings	X	√	‡		
Monitoring & Control	Ramp Rate Control				‡ (P1)	‡
	Communication Interface			‡	‡ (P2)	‡
	Disable Permit Service (Remote Shut-Off, Remote Disconnect/Reconnect)			‡	‡ (P3)	‡
	Limit Active Power			‡	‡ (P3)	
	Monitor Key DER Data			‡	‡ (P3)	
Bulk System Reliability & Frequency Support	Frequency Ride-Through (FRT)	X	√	‡	‡ (P1)	‡
	Rate-of-Change-of-Frequency Ride-Through			‡	!!!	!!!
	Voltage Ride-Through (VRT)	X	√	‡	‡ (P1)	‡
	VRT of Consecutive Voltage Disturbances			‡	!!!	!!!
	Voltage Phase Angle Jump Ride-Through			‡	!!!	!!!
	Dynamic Voltage Support during VRT			√	[‡ (P3)]	
	Frequency-Watt	X	√	‡	‡ (P3)	‡
Legend:	X Prohibited, √ Allowed by Mutual Agreement, ‡ Capability Required					
	[…] Subject to clarification of the technical requirements and use cases, !!! Important Gap					

© 2020 Electric Power Research Institute, Inc. All rights reserved.

The DER Performance Capability & Functional Settings Challenge

- Central database(s)
  - Includes only public, non-proprietary information otherwise available in utility interconnection documents
  - EPRI: https://dersettings.epri.com
- EPRI Phase 1 (2019):
  - Storage of *.csv files + metadata, search functionality
  - Need for external DER Settings Form (Excel) to validate settings and create *.csv files
- EPRI Phase 2 (2020+):
  - Verification of uploaded settings
  - Data mining, visualization



© 2020 Electric Power Research Institute, Inc. All rights reserved.

Anticipated Scope of EPRI's DER Performance Capability and Settings Database

Long-term

IA-URP
(site specific)

Utility-Required Profile for Specific Site
- Included in site-specific interconnection agreement (IA)
- May result from site-specific interconnection screenings

Mid-term

DU-URP
(distribution utility specific)

Utility-Required Profile for Distribution Service Area
- Included in interconnection agreement template
- Specific to Distribution Utility's practices, e.g., automatic re-closing, distribution circuit characteristics, operating practices

Near-term

Regional-URP[1]
(state-wide or similar)

Utility-Required Profile for Region and/or ISO/RTO Reliability Region
- Consideration of distribution and bulk system impacts.
- May include some settings other than the SRD's default values

Adopted SRD[1] with Default Values
(state-wide or similar)

Source Requirements Document
- Preferably IEEE Std 1547-2018
- Otherwise: CAR21, HR14H, etc.

Database Scope



https://dersettings.epri.com/

[1] Based on decision by Authority Governing Interconnection Requirements (AGIR), may be a public utilities commission or similar

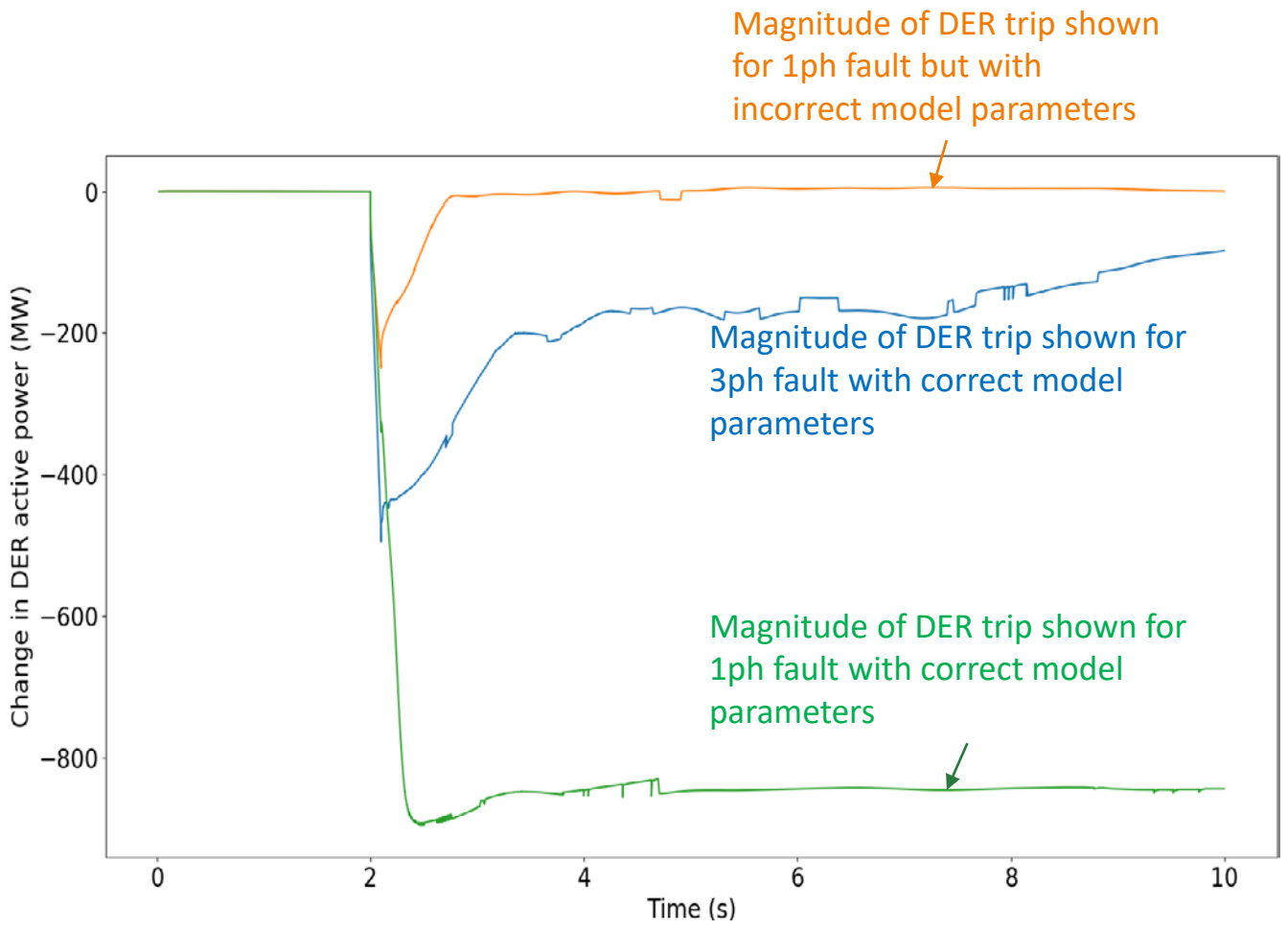
© 2020 Electric Power Research Institute, Inc. All rights reserved.

Generic parameter estimation for DER_A model

- Correct parameterization of the DER_A model is crucial to obtain an accurate picture of system behavior.

How to obtain generic parameter values for the model for a variety of geographic terrain and load profiles such as:

- Urban location, commercial load
- Urban location, residential load
- Rural location, agricultural load
- Rural location, residential load



© 2020 Electric Power Research Institute, Inc. All rights reserved.

EPRI Project 1: Inverter-Based Resources Modeling and Model Validation Using Field Measurements with Focus on Bulk Power System Impacts

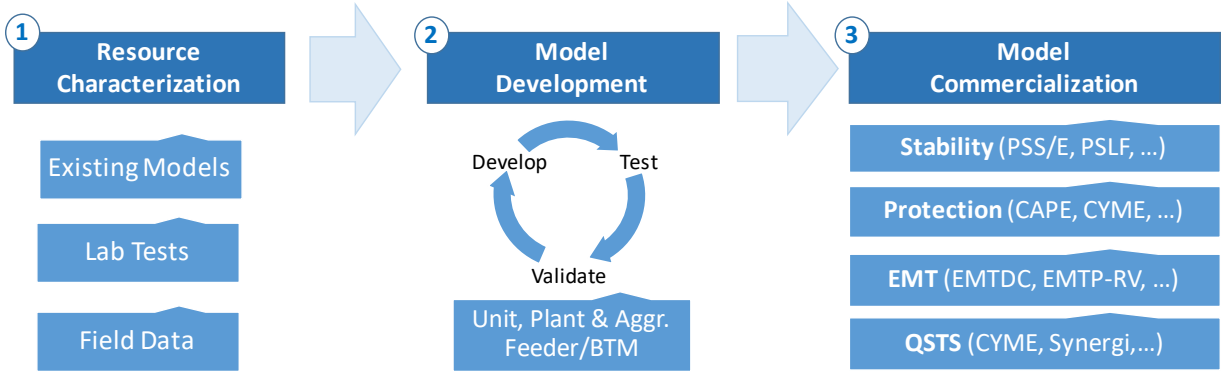
PROGRAM	40/173
PROJECT	16/3
TASK FORCE	MOD
COORDIN.	174/200

Start Date: Q2/2020, Duration: 3 years

R&D Goal

Leverage the DOE PV-MOD work to help utilities understand, test, validate, and adopt the models to improve system reliability for systems with high PV penetration

This supplemental project contributes to the $1.5M committed EPRI cost-share for the DOE PV-MOD award.



R&D Approach

- Scope includes protection, planning, and power quality models of both large-scale renewables and aggregate distributed energy resources
- Provide guidance on data collection process for field measurements
- Validate all developed models against laboratory* & field measurement disturbances; including analysis of events identified by utilities
- Help planners to gain confidence in the models by providing technical insights and guidance on how to use them in utilities' simulation platforms
- Ensure utility planners are vested in EPRI's existing vendor engagement processes to transfer the new models to commercial tool model libraries

* Leveraging joint P173/P174/P200 supplemental (3002014731) and DOE PV-MOD project

Deliverables

Deliverables are aligned to the DOE PV-MOD SOPO

- [Technical Updates] Model specs & validation
- [Webcasts] Quarterly AdvMtg & Updates

Technical Contacts

- Jens C. Boemer, +1 206.471.1180 | jboemer@epri.com
- Anish Gaikwad, +1 865.218.8040 | agaikwad@epri.com
- Aminul Huque, +1 865.218.8051 | mhuque@epri.com

© 2020 Electric Power Research Institute, Inc. All rights reserved.

Committed

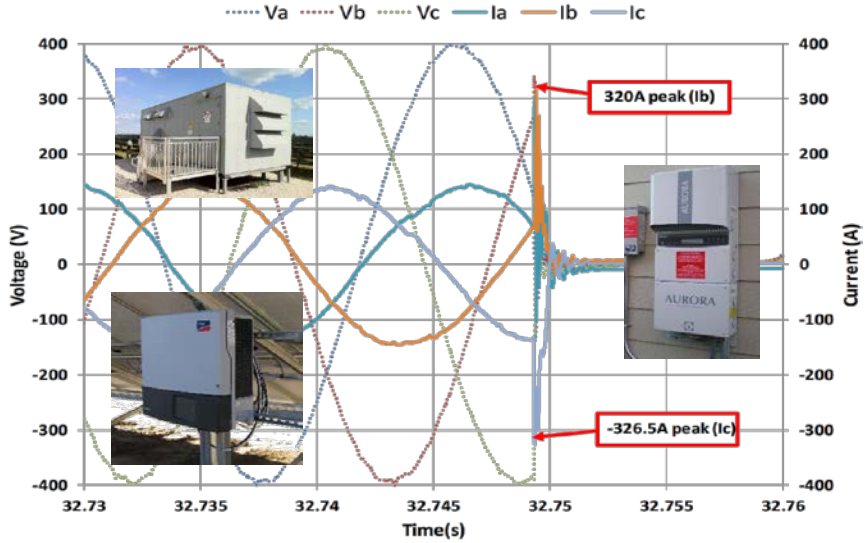
EPRI Project 2: DER Dynamic Response Characterization for Protection, Planning, and Power Quality

Objectives and Scope

- Expand industry knowledge of inverter dynamic response to grid disturbances
- Accelerate development of distribution dynamic models, evaluate and improve existing transmission aggregate DER models, and
- Identify critical parameters and ranges for sensitivity analysis.

Value

- Enhanced knowledge of commercial inverters' dynamic behavior:
  - Response to grid fault (L-L, L-L-G, L-G, and 3-phase)
  - Short-circuit current magnitude, duration, and phase
  - Active/reactive current during voltage and frequency fault ride through
  - Response to phase shift and frequency change
  - Response to single phase opening
  - Impact of out-of-phase reclosing for immunity
  - Power quality and bulk system impacts of active islanding detection
  - Reconnection time and resynchronization characteristics after trip
- Validation and improvement of existing and development of new models for protection, planning, and power quality studies.



Schedule and Cost

- Project beginning Q2 2020; Duration: 24 months

Technical Contacts

Aminul Huque, mhuque@epri.com, (865) 218-8051

Sean McGuinness, smcguinness@epri.com , 704.595.2981

Anish Gaikwad, agaikwad@epri.com , 865.218.8040

SPN Number: 3002014731

Narrow the uncertainty of inverter-based DER performance under abnormal and dynamic grid conditions.

© 2020 Electric Power Research Institute, Inc. All rights reserved.

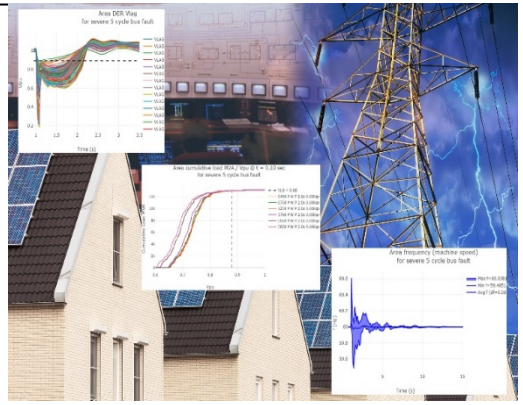
EPRI Project 3: Framework for Aggregate DER Data Pre-Processing for Transmission Planning Studies

PROGRAM	40/173
PROJECT	16/3/8
TASK FORCE	MOD
COORDIN.	174/ENV

R&D Goal

The primary R&D goal is to facilitate the entering of parameters representing the aggregate DER capacity values and performance / functional settings for transmission planning studies with DER. Among others, the framework will be capable to distinguish the amount of legacy DER (compliant to IEEE Std 1547-2003) from modern DER (compliant to IEEE Std 1547-2018) and may be linked to EPRI's DER Performance and Settings Database that is currently under development.

Maintain bulk system reliability with large amounts of distributed energy resources.



R&D Approach

- Processing of postal-code specific DER adoption forecast data based on socio-economic datasets (P174D R&D)
- Processing of distribution grid model and geographic information system (GIS) datasets
- Processing of other datasets, e.g., state databases for DER like the California Solar Energy Statistics (https://www.californiasolarstatistics.ca.gov/)

Deliverables

- [Software] Macro-Enabled Excel Spreadsheet
- [PowerPoint] Project Results Summary

- Jens C. Boemer (Project Manager & Lead)
  +1 206.471.1180 | jboemer@epri.com
- Deepak Ramasubramanian (Technical Support)
  +1 865.218.8178 | dramasubramanian@epri.com
- Steven Coley (Technical Support)
  +1 615-542-2882 | scoley@epri.com

Please answer polling question to indicate interest

© 2020 Electric Power Research Institute, Inc. All rights reserved.

NPCC Regional Standards Committee Meeting #20-2

DER Forum
Agenda Item 16.4

May 13-14, 2020

DERs Prompting More EDC and TO Coordination

EVERSOURCE ENERGY

- DERs are blurring the line between Transmission Interconnections and Distribution Interconnections
  - Significant increase in DER Transmission System Impact Studies
  - Numerous Eversource stations expected to experience Reverse Power Flow
- An increasingly relevant way for EDCs and TOs to facilitate DER development is to assist developers with making informed decisions
  - Regarding the regulatory jurisdiction of their proposed projects
  - Developing customer facing technology solutions such as Hosting Capacity Maps
  - Implementing expedited study processes for projects that have minimal impact to reliability or operations.
- Increasing amount of DERs intend to participate in wholesale markets
  - Improved coordination with ISO NE when performing capacity market qualification reviews

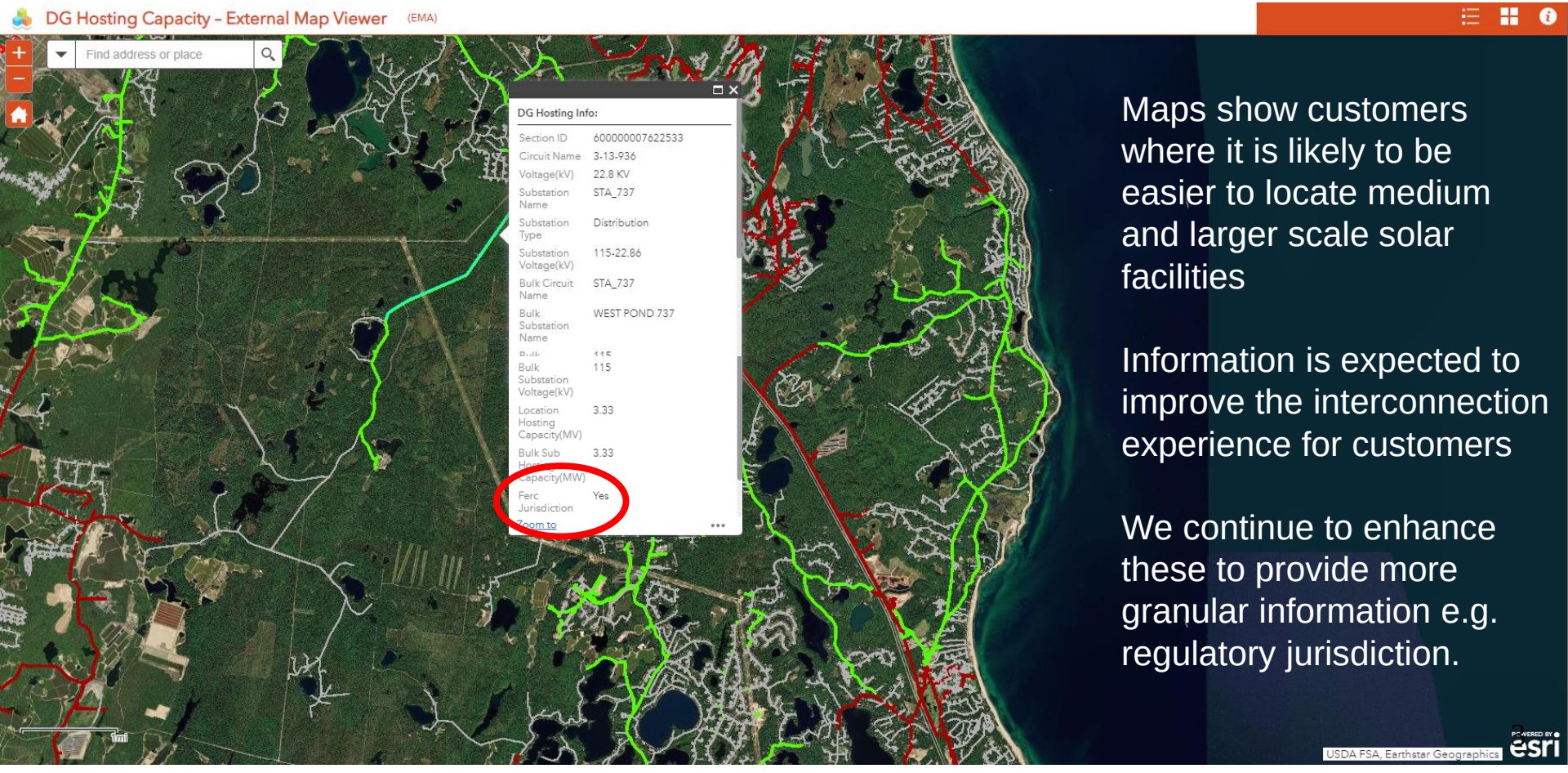
Eversource Quick Stats

- Eversource strives to promote DER growth and implemented internal D and T coordination 5 years ago
- **2,101:** Eversource owns approximately 2,010 distribution facilities
- **310:** Of which, roughly 310 are dual-use facilities (i.e., used for wholesale and retail sales)
- **50%:** The number of dual-use facilities is expected to increase by 50 percent year-over-year
- When a DER is proposing to interconnect to a dual-use distribution facility and make wholesale sales itself, it needs to submit an interconnection request to ISONE

Hosting Capacity Maps 2.0

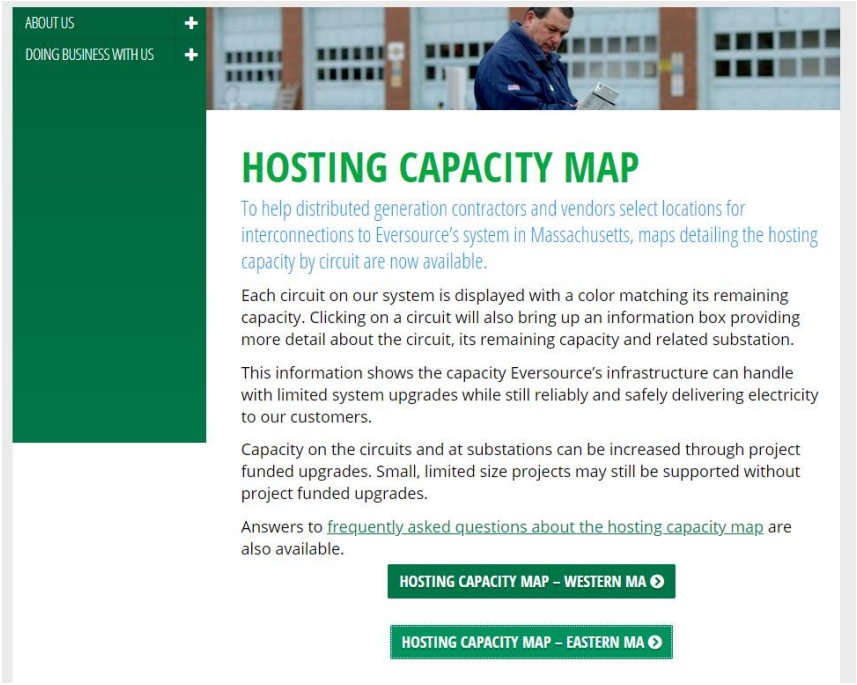
EVERSOURCE ENERGY

- Eversource's DER Hosting Capacity Maps now include distribution facility regulatory jurisdiction



Website Links

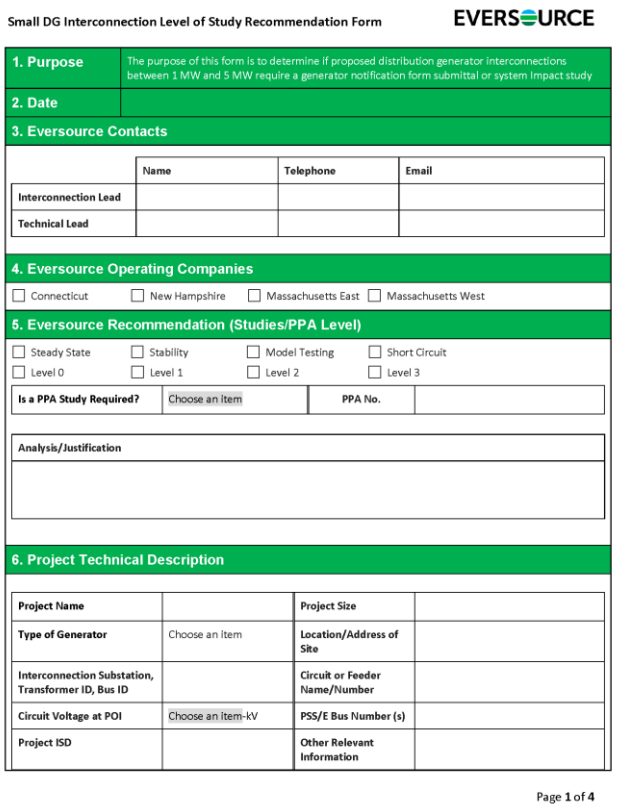
- Eversource's Hosting Capacity Maps publicly available here: https://www.eversource.com/content/ct-c/about/about-us/doing-business-with-us/builders-contractors/interconnections/massachusetts-application-to-connect/hosting-capacity-map



ISONE I.3.9 Level 0 Screening

- The Proposed Plan Application requirements for DERs sized >1MW and < 5 MW are subject to ISONE discretion (per Planning Procedure 5-1)

- To expedite the process and facilitate ISONE's determination, Eversource developed and uses a screening document to provide more information to help justify a Level 0 Notification Form



Small DG Interconnection Level of Study Recommendation Form

EVERSOURCE

1. Purpose	The purpose of this form is to determine if proposed distribution generator interconnections between 1 MW and 5 MW require a generator notification form submittal or system impact study
2. Date	

3. Eversource Contacts

	Name	Telephone	Email
Interconnection Lead			
Technical Lead			

4. Eversource Operating Companies

☐ Connecticut ☐ New Hampshire ☐ Massachusetts East ☐ Massachusetts West

5. Eversource Recommendation (Studies/PPA Level)

☐ Steady State ☐ Stability ☐ Model Testing ☐ Short Circuit
☐ Level 0 ☐ Level 1 ☐ Level 2 ☐ Level 3

Is a PPA Study Required?	Choose an item	PPA No.	

Analysis/Justification

6. Project Technical Description

Project Name		Project Size	
Type of Generator	Choose an item	Location/Address of Site	
Interconnection Substation, Transformer ID, Bus ID		Circuit or Feeder Name/Number	
Circuit Voltage at POI	Choose an item-kV	PSS/E Bus Number (s)	
Project ISD		Other Relevant Information	

Page 1 of 4

Automatic Underfrequency Load Shedding and Distributed Energy Resources

Northeast Power Coordinating Council
Regional Standards Committee DER Forum

Dan Kopin
Utility Services

May 2020

Agenda

- Premise
- “Friendly Neighborhood Utility” – *Hypothetical*
  - NERC Standard PRC-006
  - SPIDER Working Group Reliability Guideline
  - Hosting Capacity Analysis
- ERCOT Market Notice & Proposal

Premise

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Guideline Key Takeaways

- ***Aggregate*** amounts of DER can and will impact the BPS
  - NERC Goal: provide support where needed in this area; ensure BPS reliability

Source: NERC (2020)

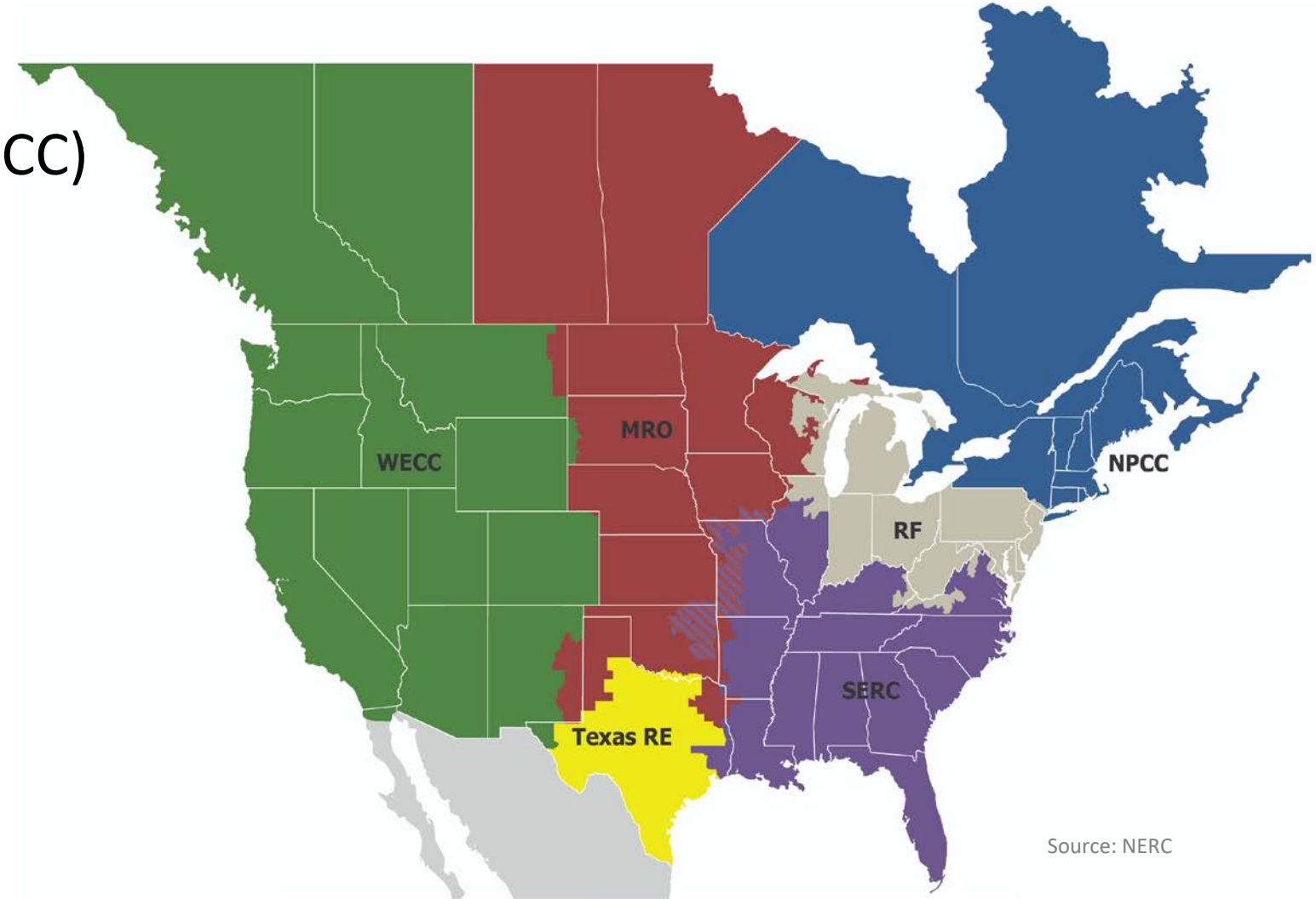
“Friendly Neighborhood Utility”

- Eastern Interconnection



“Friendly Neighborhood Utility”

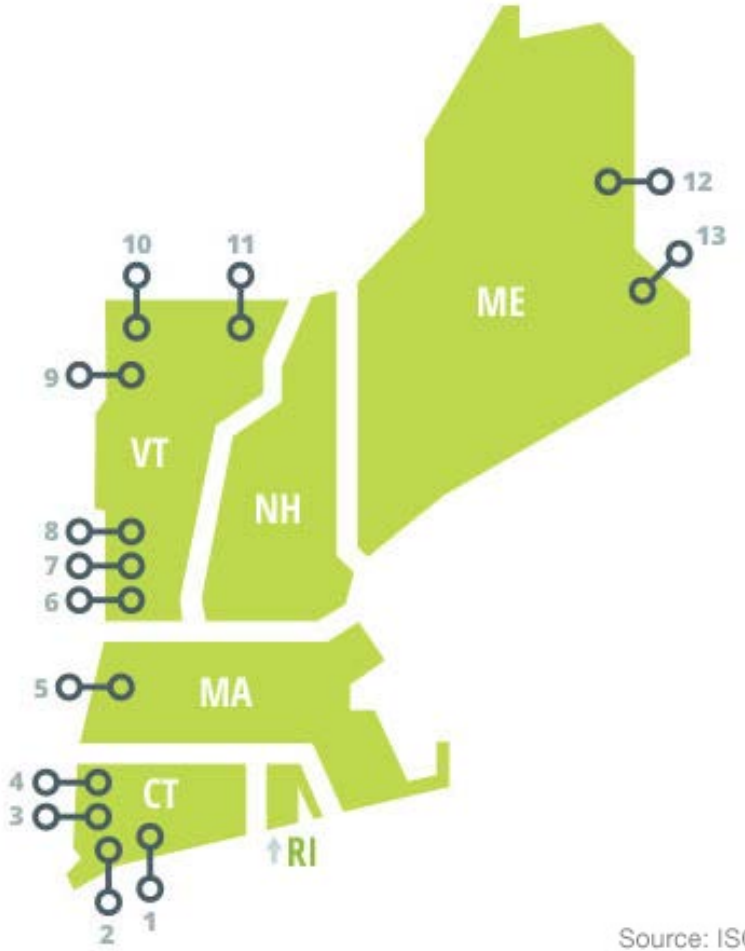
- Eastern Interconnection
- Northeast Power Coordinating Council (NPCC)



Source: NERC

“Friendly Neighborhood Utility”

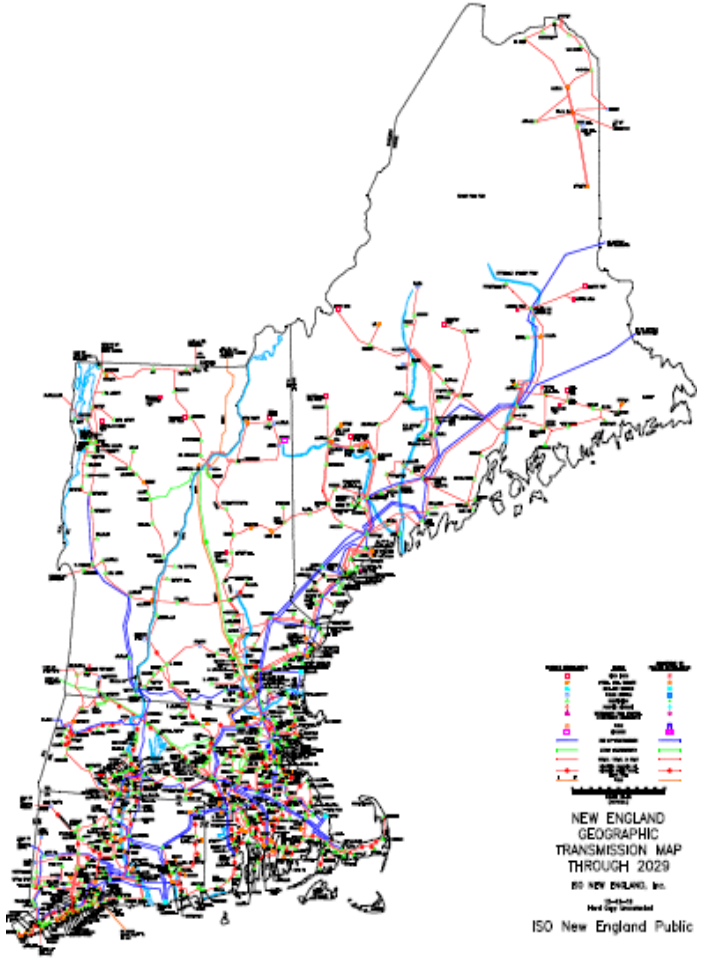
- Eastern Interconnection
- Northeast Power Coordinating Council (NPCC)
- ISO New England Balancing Authority Area



Source: ISO New England

“Friendly Neighborhood Utility”

- Eastern Interconnection
- Northeast Power Coordinating Council (NPCC)
- ISO New England Balancing Authority Area
- NERC-registered Distribution Provider (DP)
  - Connected at 115 kilovolts (kV)
  - Peak of 100 megawatts (MW)

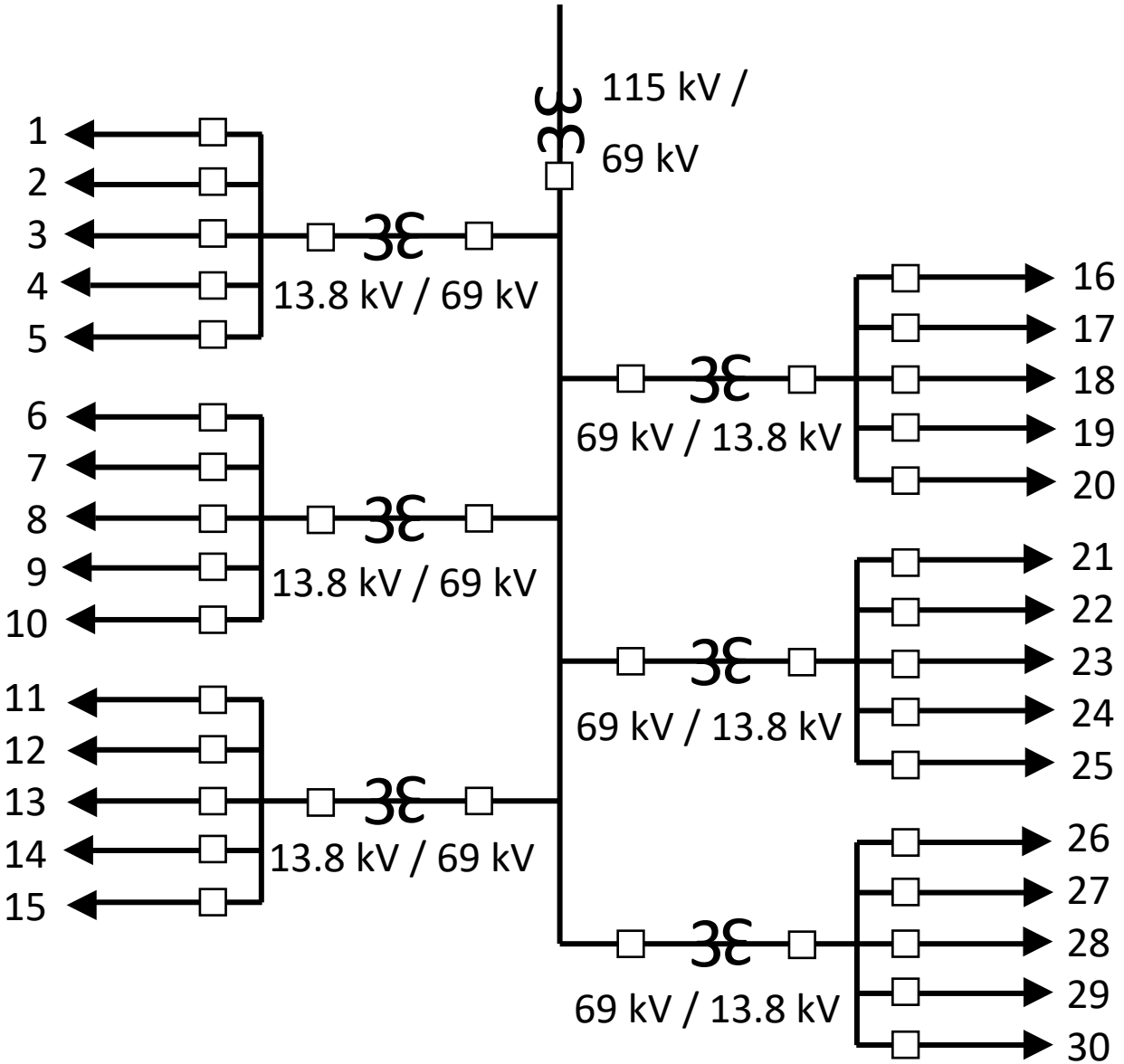


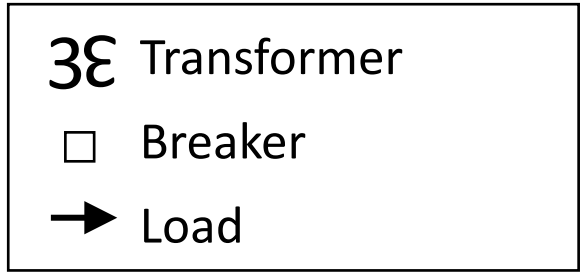
“Friendly Neighborhood Utility”

- Eastern Interconnection
- Northeast Power Coordinating Council (NPCC)
- ISO New England Balancing Authority Area
- NERC-registered Distribution Provider (DP)
  - Connected at 115 kilovolts (kV)
  - Peak of 100 megawatts (MW)
- Applicable to NERC Standards
  - FERC Order No. 693 (2007)
  - FERC Order No. 773 (2012)



“Friendly Neighborhood Utility”





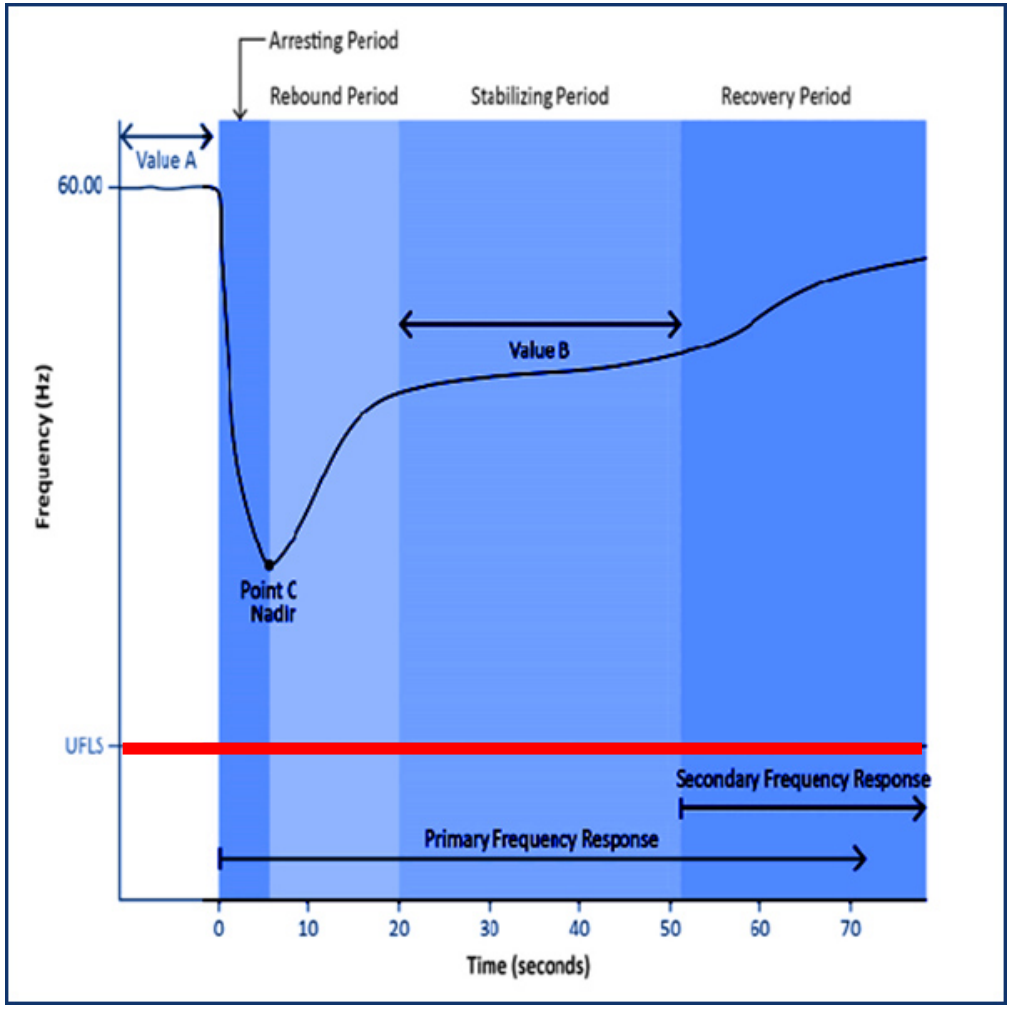
- Eastern Interconnection
- NPCC
- ISO New England
- NERC-registered Distribution Provider
  - 115 kV Connection
  - 100 MW Peak
- **1 BES/BPS Interface**
- **6 BPS/Distribution Interfaces**
- **30 Feeders**

PRC-006

- As a DP, “Friendly Neighborhood Utility” is applicable to PRC-006 *Automatic Underfrequency Load Shedding*.
  - Given that this “Friendly Neighborhood Utility” hypothetical is in NPCC, specifically PRC-006-NPCC-1. Otherwise, DPs and DP-UFLS Only Entities are applicable to either PRC-006-3 or PRC-006-SERC-02.
- What is Underfrequency Load Shedding (UFLS)?

PRC-006

"Reliability is threatened when a large electric generator(s) disconnects from the power system because the loss of generation causes an immediate decline in power system frequency. If the loss of generation is large enough and the remaining, still-connected generators do not respond and rapidly arrest the decline in frequency, power system frequency may decline below established, safe operating bounds and trigger automatic, emergency load shedding to avoid a cascading blackout" – LBNL (2018)



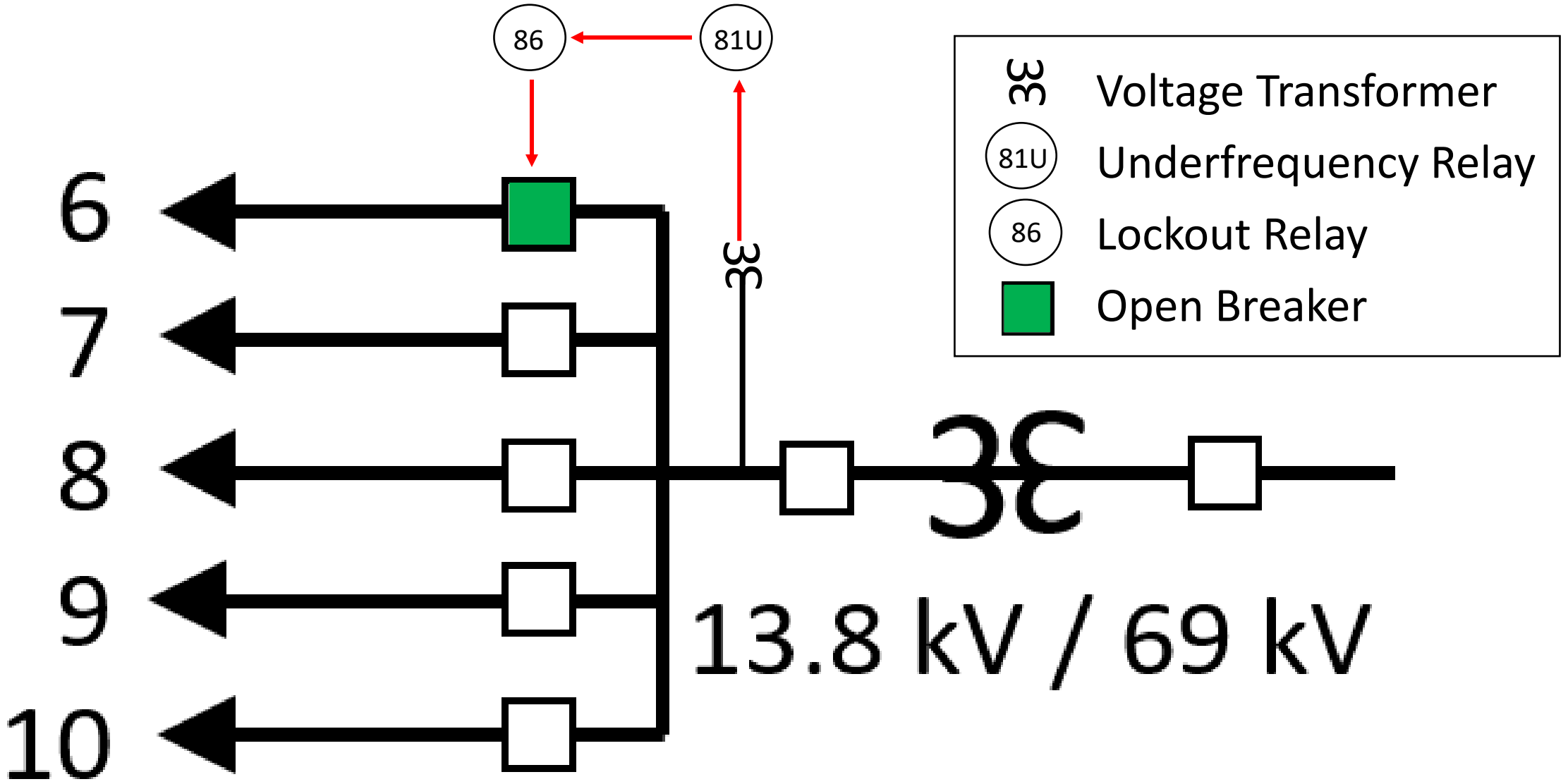
= Automatic Underfrequency Load Shedding

PRC-006

- FERC Order No. 763

  "The UFLS program addressed in Reliability Standard [PRC-006] is important to arresting declining frequency and assisting recovery of frequency following system events that lead to system instability, which can result in a blackout. Accordingly, the Reliability Standard is necessary for reliability because UFLS is used in extreme conditions to stabilize the balance between generation and load after an electrical island has been formed, dropping enough load to allow frequency to stabilize within the island."

PRC-006


86
81U
6
7
8
9
10
13.8 kV / 69 kV
Voltage Transformer
Underfrequency Relay
Lockout Relay
Open Breaker

PRC-006-NPCC-1
Automatic Underfrequency Load Shedding

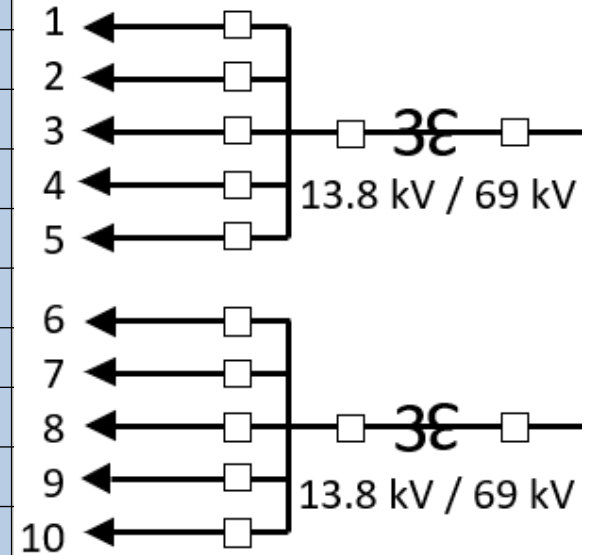
	Peak ≥ 100 MW		***50 MW ≤ Peak < 100 MW***		***25 MW ≤ Peak < 50 MW***	
Trip Setting (Hz)	Load Shed	Cumulative Load Shed	Load Shed	Cumulative Load Shed	Load Shed	Cumulative Load Shed
59.5	6.5-7.5%	6.5-7.5%	14-25%	14-25%	28-50%	**28-50%**
59.3	6.5-7.5%	13.5-14.5%				
59.1	6.5-7.5%	20.5-21.5%	14-25%	**28-50%**		
58.9	6.5-7.5%	27.5-28.5%				
59.5 (10s)	2-3%	**29.5-31.5%**				

PRC-006-NPCC-1
Automatic Underfrequency Load Shedding

Entity Name:	Projected DP 2025 Peak Load (MW)	UFLS Feeder ID	Trip Setting	Feeder Load Tripped (MW)	% of Peak
"Friendly Neighborhood Utility"	100	1	59.5	3.5	3.5
		2	59.5	3.5	3.5
		3	59.3	3.5	3.5
		4	59.3	3.5	3.5
		5	59.1	3.5	3.5
		6	59.1	3.5	3.5
		7	58.9	3.5	3.5
		8	58.9	3.5	3.5
		9	59.5 (10s)	1	1
		10	59.5 (10s)	1	1
				30	30

PRC-006-NPCC-1
Automatic Underfrequency Load Shedding

Entity Name:	Projected DP 2025 Peak Load (MW)	UFLS Feeder ID	Trip Setting	Feeder Load Tripped (MW)	% of Peak
"Friendly Neighborhood Utility"	100	1	59.5	3.5	
		2	59.5	3.5	
		3	59.3	3.5	
		4	59.3	3.5	
		5	59.1	3.5	
		6	59.1	3.5	
		7	58.9	3.5	
		8	58.9	3.5	
		9	59.5 (10s)	1	
		10	59.5 (10s)	1	
				30	30



PRC-006-NPCC-1
Automatic Underfrequency Load Shedding

Entity Name:	Projected DP 2025 Peak Load (MW)	UFLS Feeder ID	Trip Setting	Feeder Load Tripped (MW)	% of Peak	DER (MW)
"Friendly Neighborhood Utility"	100	1	59.5	3.5	3.5	0
		2	59.5	3.5	3.5	0
		3	59.3	3.5	3.5	0
		4	59.3	3.5	3.5	0
		5	59.1	3.5	3.5	0
		6	59.1	3.5	3.5	0
		7	58.9	3.5	3.5	0
		8	58.9	3.5	3.5	0
		9	59.5 (10s)	1	1	0
		10	59.5 (10s)	1	1	0
				30	30	0

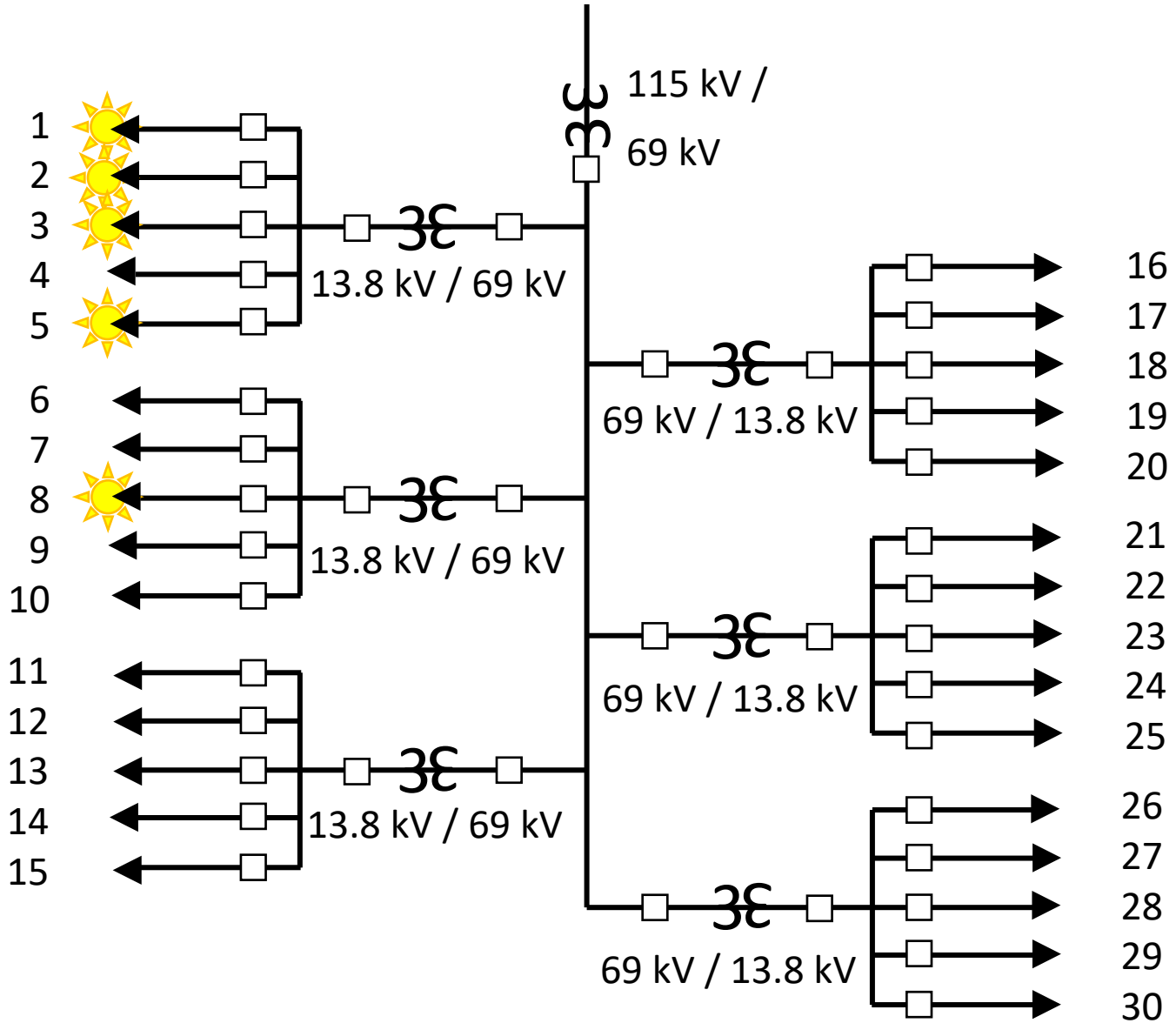
PRC-006-NPCC-1
Automatic Underfrequency Load Shedding

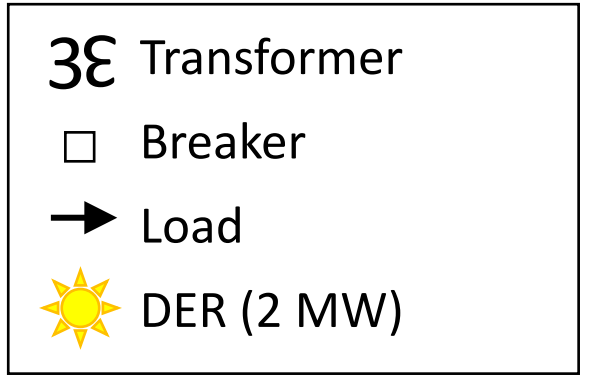
Entity Name:	Projected DP 2025 Peak Load (MW)	UFLS Feeder ID	Trip Setting	Feeder Load Tripped (MW)	% of Peak	DER (MW)
"Friendly Neighborhood Utility"	95	1	59.5	2.5	2.6	1
		2	59.5	2.5	2.6	1
		3	59.3	2.5	2.6	1
		4	59.3	3.5	3.7	0
		5	59.1	2.5	2.6	1
		6	59.1	3.5	3.7	0
		7	58.9	3.5	3.7	0
		8	58.9	2.5	2.6	1
		9	59.5 (10s)	1	1.1	0
		10	59.5 (10s)	1	1.1	0
				25	26.3	5

PRC-006-NPCC-1
Automatic Underfrequency Load Shedding

Entity Name:	Projected DP 2025 Peak Load (MW)	UFLS Feeder ID	Trip Setting	Feeder Load Tripped (MW)	% of Peak	DER (MW)
"Friendly Neighborhood Utility"	90	1	59.5	1.5	1.7	2
		2	59.5	1.5	1.7	2
		3	59.3	1.5	1.7	2
		4	59.3	3.5	3.9	0
		5	59.1	1.5	1.7	2
		6	59.1	3.5	3.9	0
		7	58.9	3.5	3.9	0
		8	58.9	1.5	1.7	2
		9	59.5 (10s)	1	1.1	0
		10	59.5 (10s)	1	1.1	0
				20	22.2	10

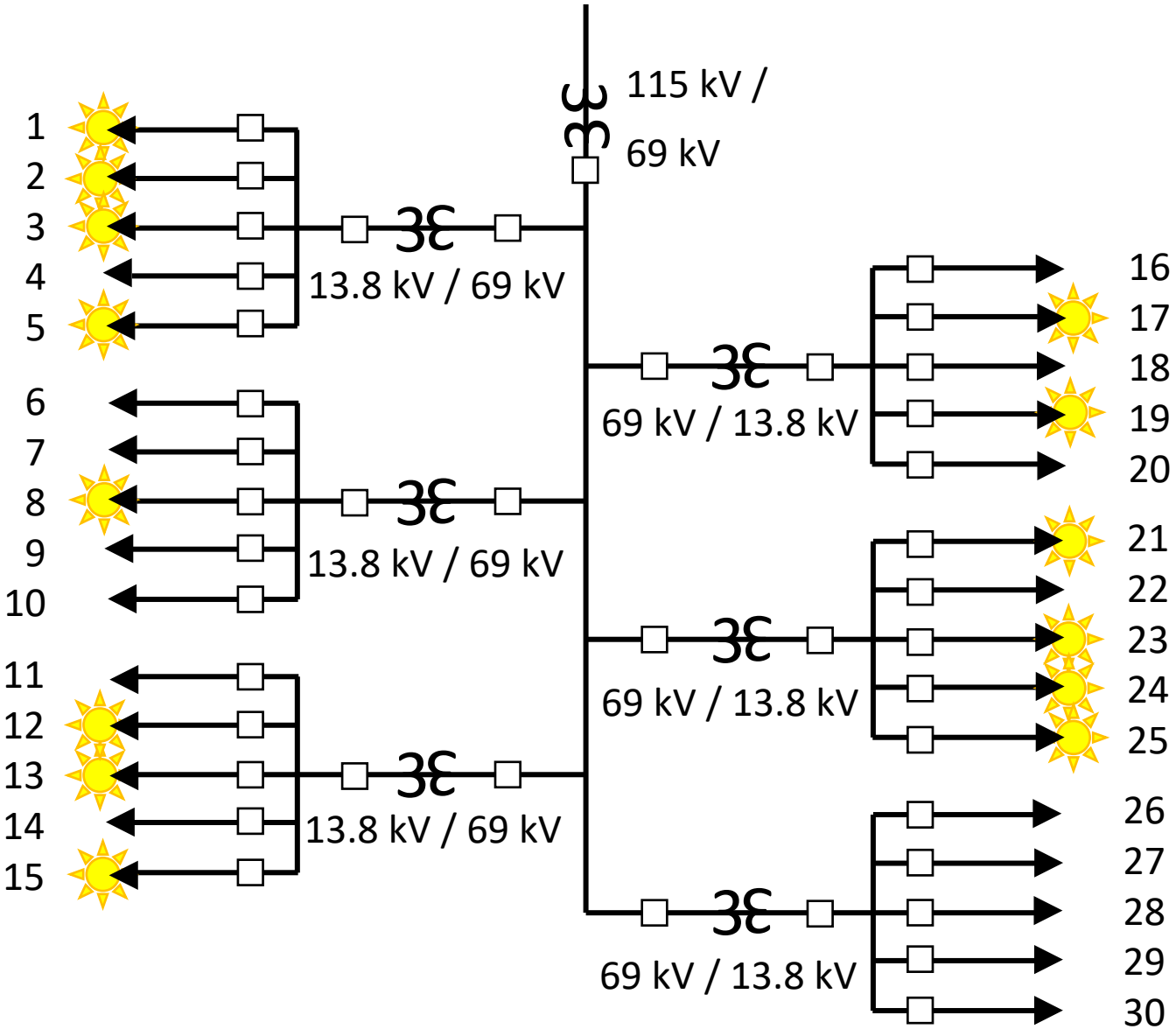
PRC-006





Which feeders are eligible for UFLS?

PRC-006



Transformer

Breaker

Load

DER (2 MW)

Which feeders are eligible for UFLS?

PRC-006
NPCC DER Guidance Document (August 2019)

"The importance of an effective automatic UFLS program cannot be overemphasized. UFLS is considered a "safety net" for the [Bulk Electric System] and a last resort."

"UFLS is primarily armed on distribution feeders, where DER is increasingly being deployed."

"As DER penetrates in the longer term it may be necessary to adopt a more flexible approach to UFLS" with real-time monitoring of feeder load.

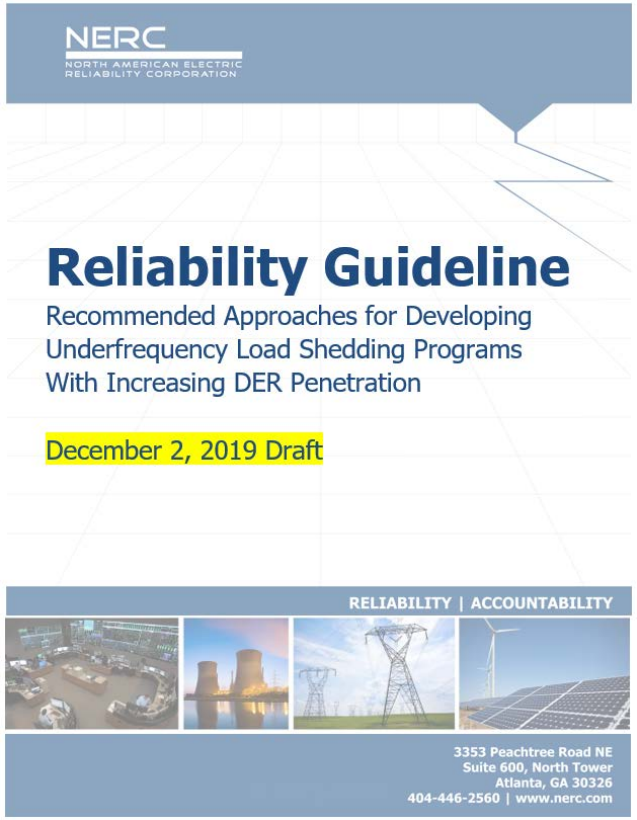
NPCC (2019)

SPIDER Working Group Reliability Guideline

Reliability Guideline: Recommended Approaches for Developing UFLS Programs with Increasing DER Penetration

Guidance on how to study UFLS programs and ensure their effectiveness with increasing penetration of DER represented.

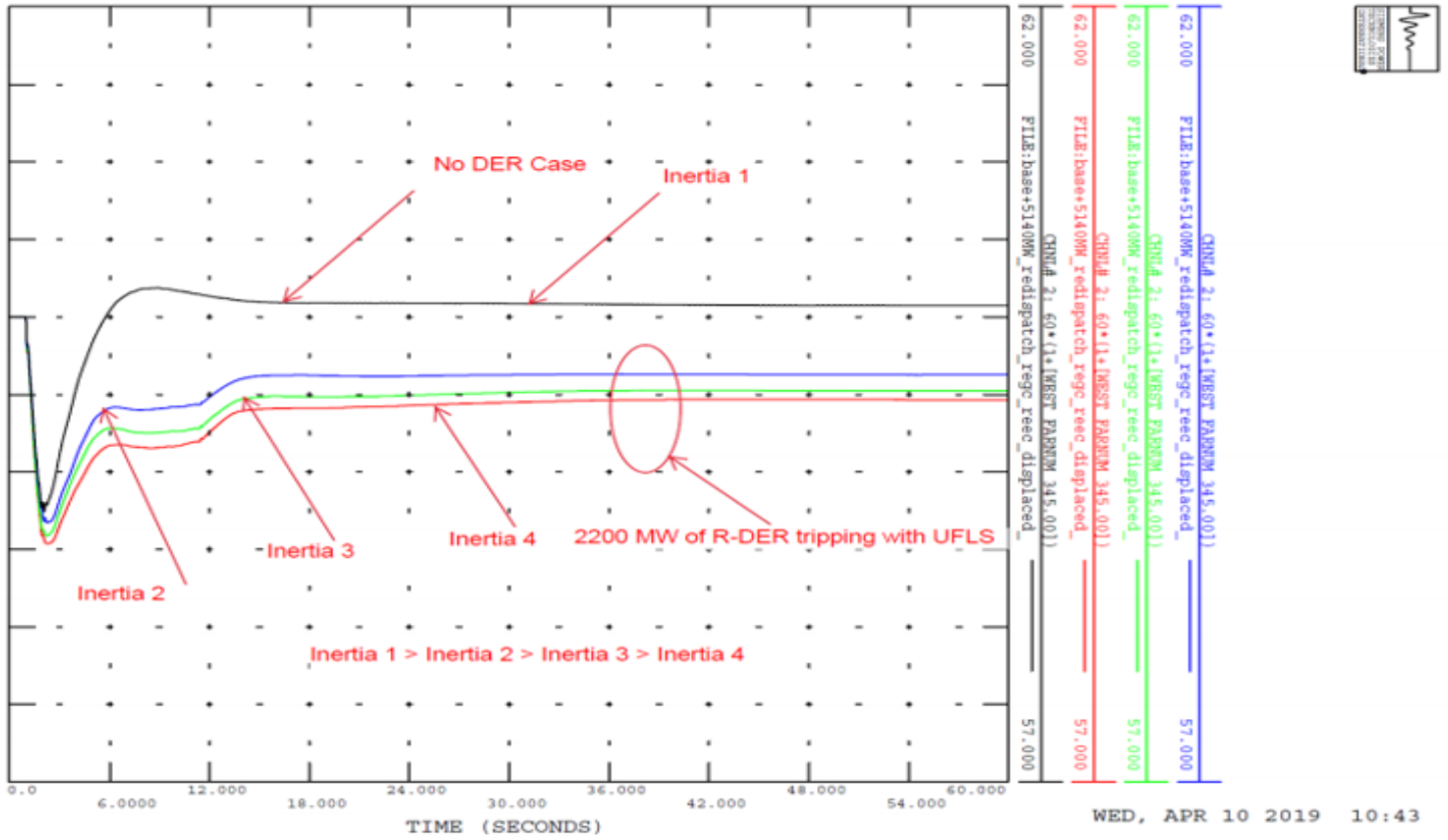
- Background
- Impacts of DER on Island-Level Frequency
- Impacts of DER on UFLS Program Design
- Recommendations



SPIDER Working Group Reliability Guideline

Impact of DER on Island-Level Frequency: Available Load Shed

ISO New England's Islanding Study – Impact of DER



ISO New England Island Frequency Performance – 60 Seconds

SPIDER Working Group Reliability Guideline

Impact of DER on UFLS Program Design: Load Selection

Hawai‘i Electric Light’s Adaptive UFLS

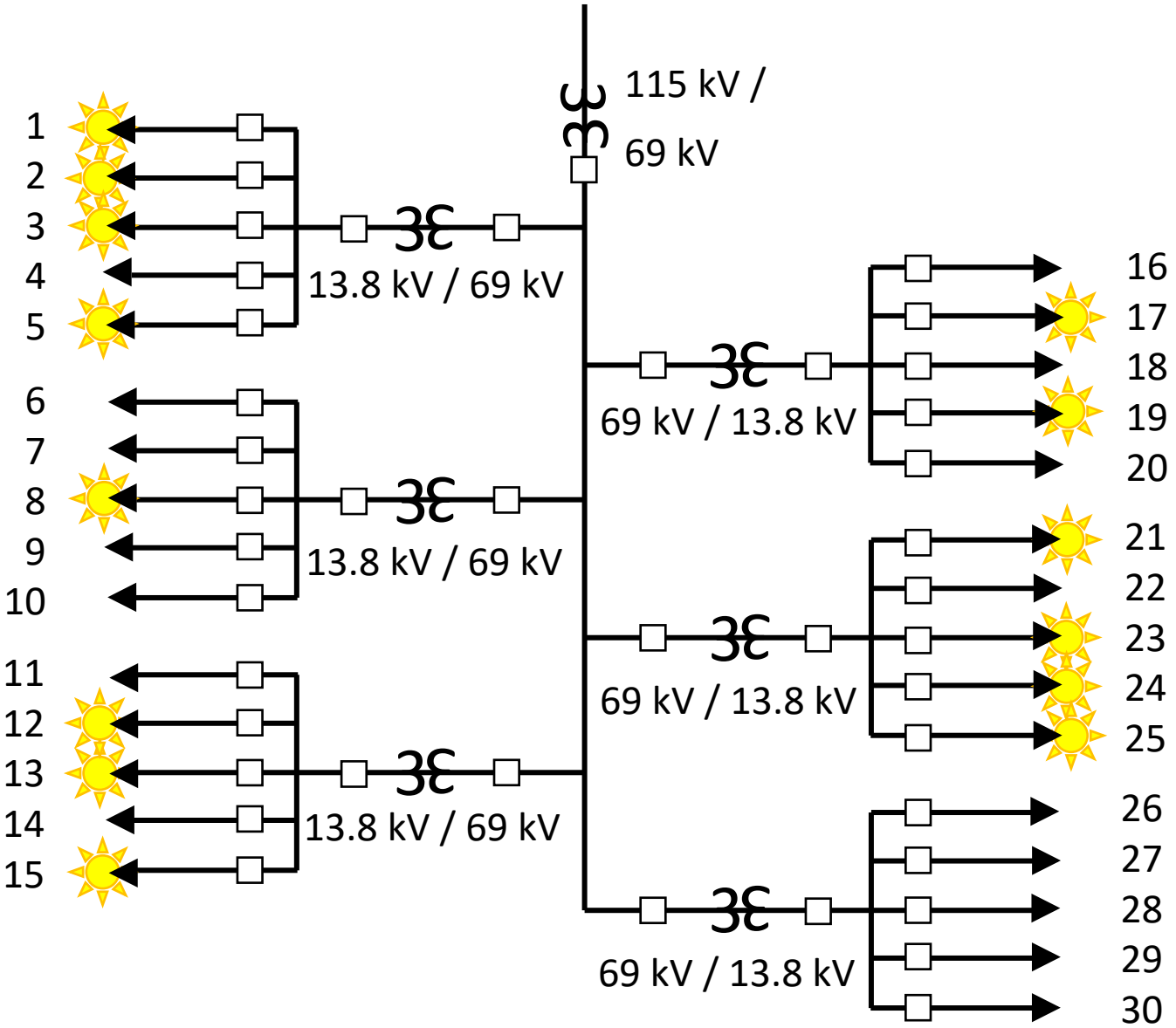
UFLS STAGE DATA

System Load: 141.853
Total Target: 112.185
Total Available: 114.292

Stage	Frequency	Percent	Target MW	Avail MW	Tol %	Tolerance	Delta MW
STAGE1	59.100	5.00	7.01154	6.82032	5.000	0.351	0.191
STAGE2	58.800	10.00	14.02308	13.83560	5.000	0.701	0.187
STAGE3	58.500	10.00	14.02308	13.34422	5.000	0.701	0.679
STAGE4	58.200	15.00	21.03462	22.24468	8.000	1.683	-1.210
STAGE5	57.900	10.00	14.02308	14.21575	8.000	1.122	-0.193
STAGE6	57.600	20.00	28.04617	25.46988	25.000	7.012	2.576
KICKER1	59.500	5.00	7.01154	6.79824	8.000	0.561	0.213
KICKER2	59.300	5.00	7.01154	6.54598	8.000	0.561	0.466

Summary Display of Hawaii Electric Light Adaptative UFLS Scheme EMS

Hosting Capacity Analysis



Transformer

Breaker

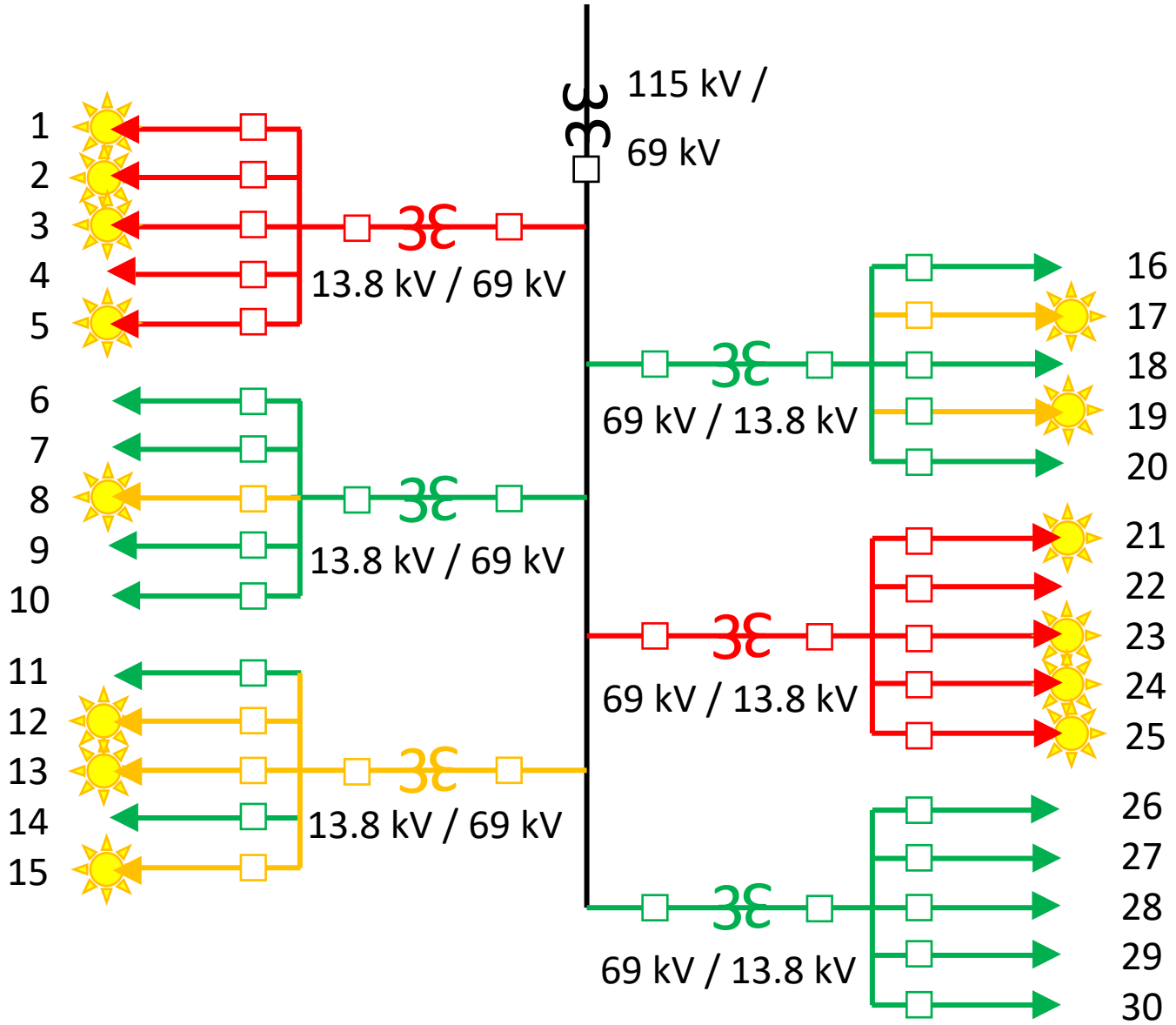
Load

DER (2 MW)

Which feeders have hosting capacity for DER?

Which feeders are eligible for UFLS?

Hosting Capacity Analysis



Transformer

Breaker

Load

DER (2 MW)

Capacity

Which feeders have hosting capacity for DER?

Which feeders are eligible for UFLS?

ERCOT Market Notice & Proposal

"ERCOT rules do not address how Transmission and/or Distribution Service Provider (TDSP) Load-shed obligations may be impacted by DGRs. If feeders that connect DGRs to the ERCOT System are disconnected during an Energy Emergency Alert (EEA), Under-Frequency Load Shed (UFLS), or Under-Voltage Load Shed (UVLS) event, the resulting unavailability of the generation can worsen an already severe reliability condition. This regulatory gap will need to be addressed by changes to ERCOT rules and possibly Public Utility Commission (PUC) rules."

ERCOT (2019)

ERCOT Market Notice & Proposal

3.8.7 Distribution Generation Resources (DGR)

(1) As a condition for the interconnection of a DGR, the affected Resource Entity, after consultation with the relevant Distribution Service Provider (DSP), shall provide documentation from the DSP to ERCOT stating that the interconnecting distribution circuit will not be disconnected as part of a manual or automatic Load-shed system during a Load shed event, including without limitation an Energy Emergency Alert (EEA) Level 3 event, an under-frequency Load shedding event, or an under voltage Load shedding event. DSPs shall ensure that Generation Resources are not connected to Load circuits subject to disconnection. If a DSP determines that the circuit to which a DGR is interconnected must be designated for Load-shed, then the DSP shall provide at least 120 days' notice of the change in designation to the Resource Entity for the DGR. The Resource Entity shall deregister the DGR by submitting an appropriate modeling change to ERCOT to be effective prior to the date on which the Load-shed designation will be effective.

ERCOT (2019)

Takeaways

- DPs are required to comply with PRC-006, regardless of DER integration levels.
- Hosting capacity analysis encourages DER integration on the same feeders that are used for UFLS, diminishing effectiveness.
- DPs require flexibility to implement UFLS programs, especially in areas with high levels of DER.
- Wholesale markets for DER are just beginning to account for UFLS requirements.
- State-level transmission/distribution planning venues are ideal for discussing and addressing these issues with stakeholders.

Thank You!
Questions?
dan.kopin@utilitysvcs.com



Autonomous Energy Systems

A vision of the future grid integrating massive amounts of distributed energy resources

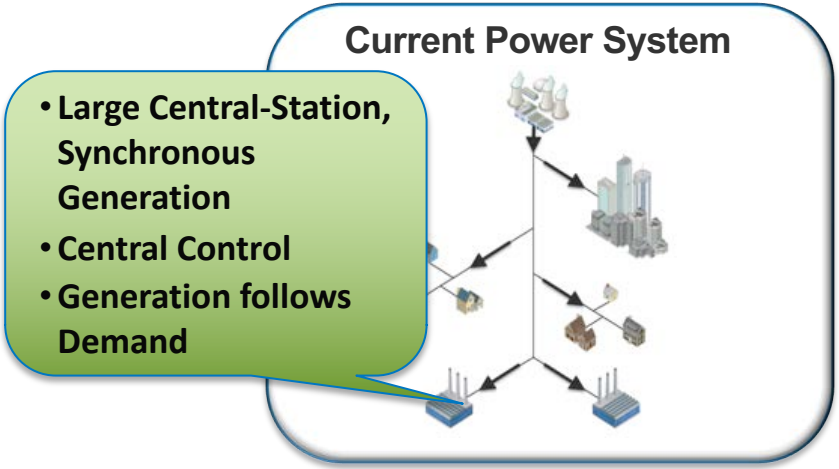
Ben Kroposki, PhD, PE, FIEEE
Director – Power Systems Engineering Center
National Renewable Energy Laboratory

May 2020

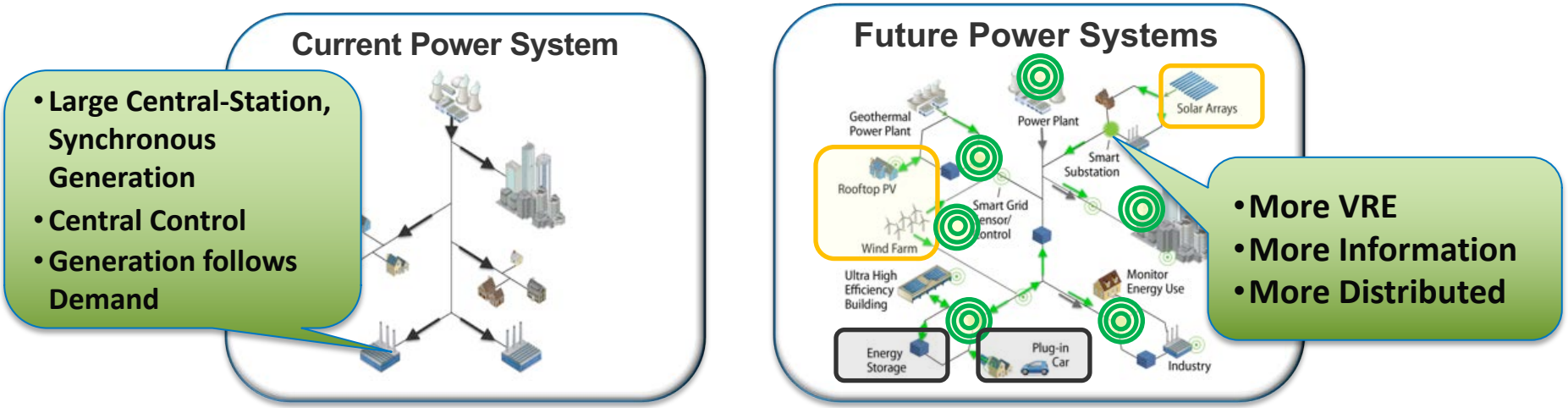
Disclaimer

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Transformation of the Power System



Transformation of the Power System



- Increasing levels of wind and solar – variable and power electronics based
- More use of Communications, Controls, Data, and Information (e.g. Smart Grids) – can have interoperability and cybersecurity issues
- Other new distributed technologies: EVs, Distributed storage, Flexible Loads
- Increasing interdependencies between electricity grids and other infrastructures
- Becoming highly distributed and more complex to operate

Is the Grid getting too complex to control?

Current Grid

Central Control
10^4 Bulk Generators

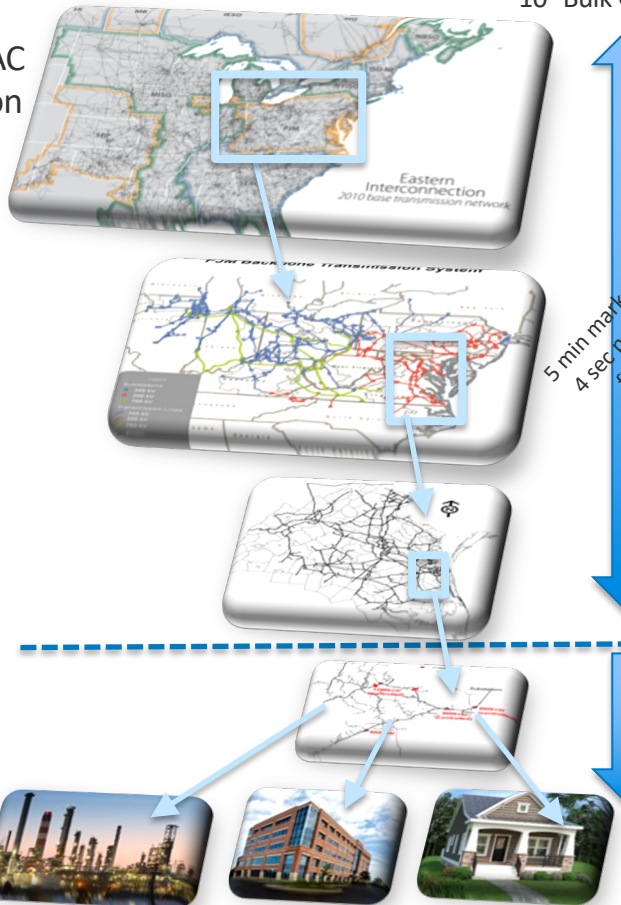
Synchronous AC Interconnection

Regional Transmission Operator -
Market/
Reliability
Coordinator

Local Utility -
Transmission/
Subtransmission/
Bulk Generation

Local Utility Distribution

Industry/
Commercial/
Residential



- 128M Households in US
- 6M Commercial buildings
- + Industry and Transportation

Is the Grid getting too complex to control?

Current Grid

Central Control
10^4 Bulk Generators

Synchronous AC Interconnection

Regional Transmission Operator -
Market/ Reliability Coordinator

Local Utility -
Transmission/ Subtransmission/ Bulk Generation

Local Utility Distribution

Industry/ Commercial/ Residential

5 min markets
4 sec power flows

Central Control ?
10^4 Bulk Generators and Storage
+
10^8 DER

- 128M Households in US
- 6M Commercial buildings
- + Industry and Transportation

Distributed, Hierarchical Control

10^8 Generators, Storage, Active Loads
1 sec optimizations at each level

Millions

1000s

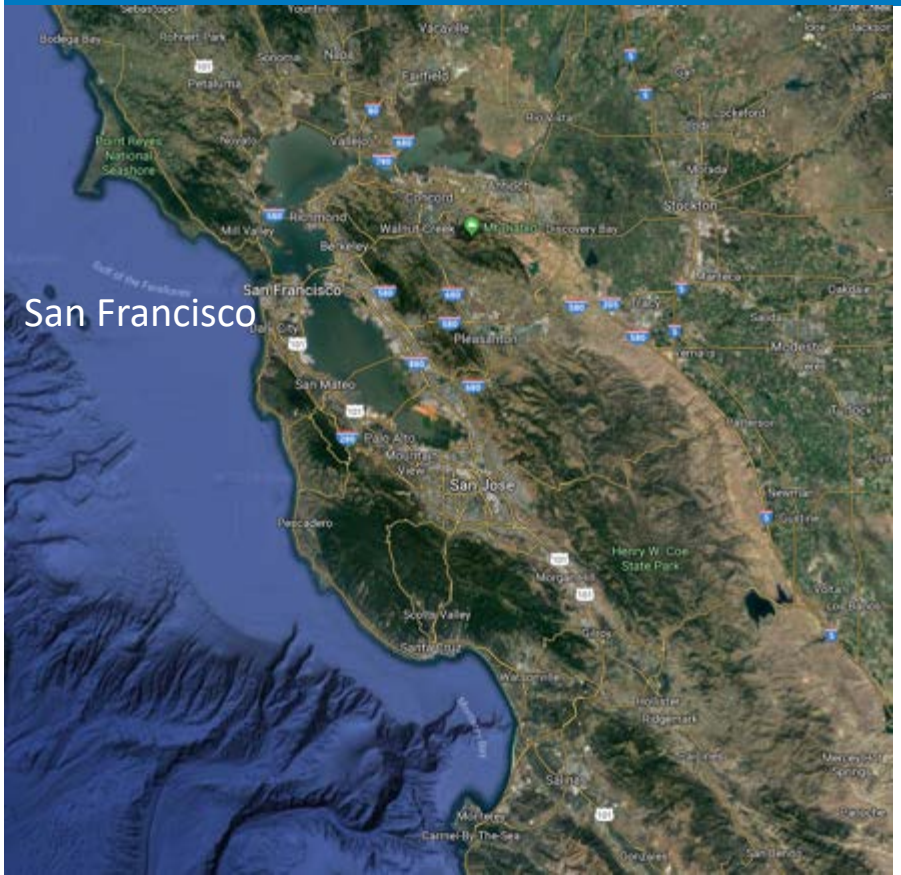
1-100

Virtual Emulation

Flatirons Campus

ESIF

What are we trying to achieve in the Autonomous Energy Systems Project?

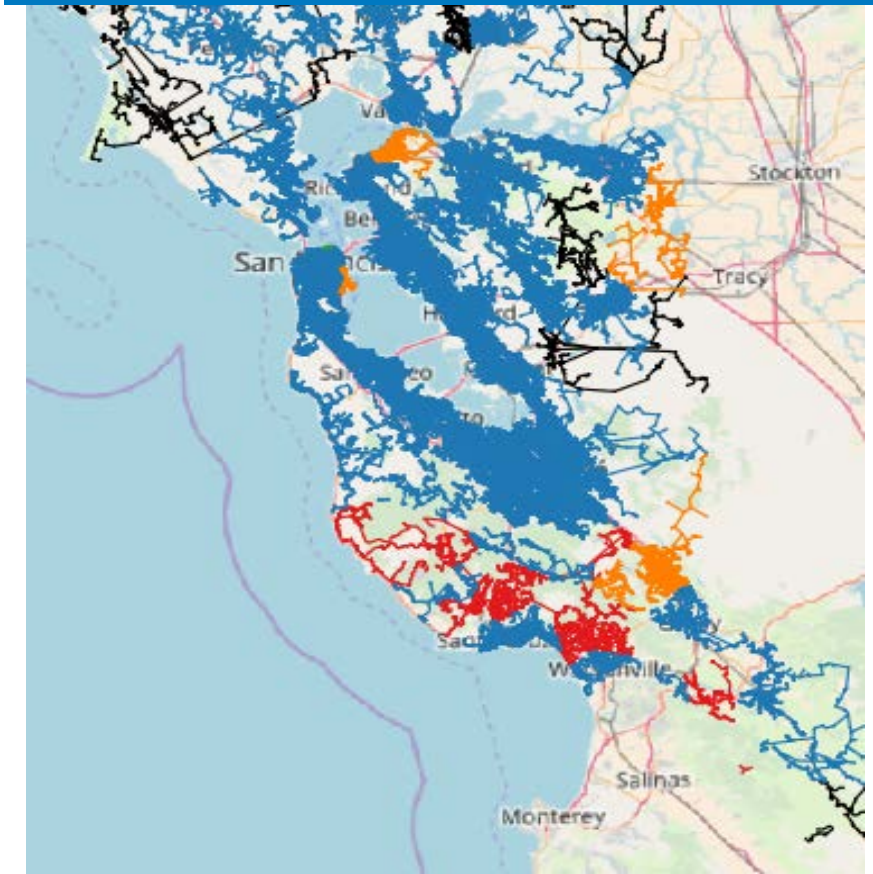


Distributed Energy Resources (DER) =

- Generation (solar, wind, fuel cells, generators)
- Storage = Batteries, Ice storage
- Loads = Buildings, Homes
- Mobility = EVs, Chargers

Optimize and control massively deployed DER in real-time.

What are we trying to achieve in the Autonomous Energy Systems Project?



Distributed Energy Resources (DER) =

- **Generation (solar, wind, fuel cells, generators)**
- **Storage = Batteries, Ice storage**
- **Loads = Buildings, Homes**
- **Mobility = EVs, Chargers**

Optimize and control massively deployed DER in real-time.

Example: SF Bay Area

- Grid has more than 10 million electric nodes at distribution level
- 4.3 million Customers – each with PV, storage, smart homes, plug-in EVs = 10-20 million controllable devices

Nobody knows how to do this!

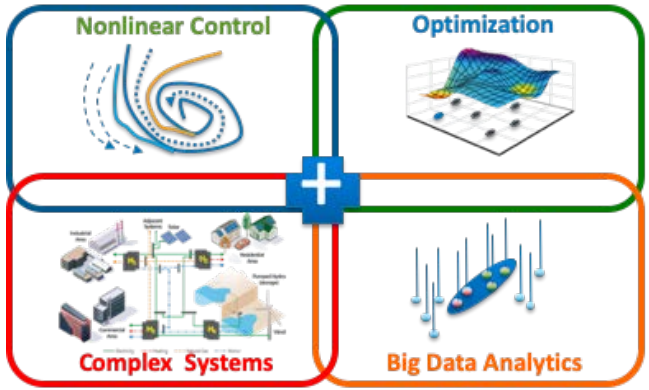
Transforming ENERGY through Autonomous Energy Systems

Home | Neighborhood | Community/Town | Large City



Develop framework to enable scalable control and optimization of all energy resources across several domains (grids, buildings, transport, renewables) and scales

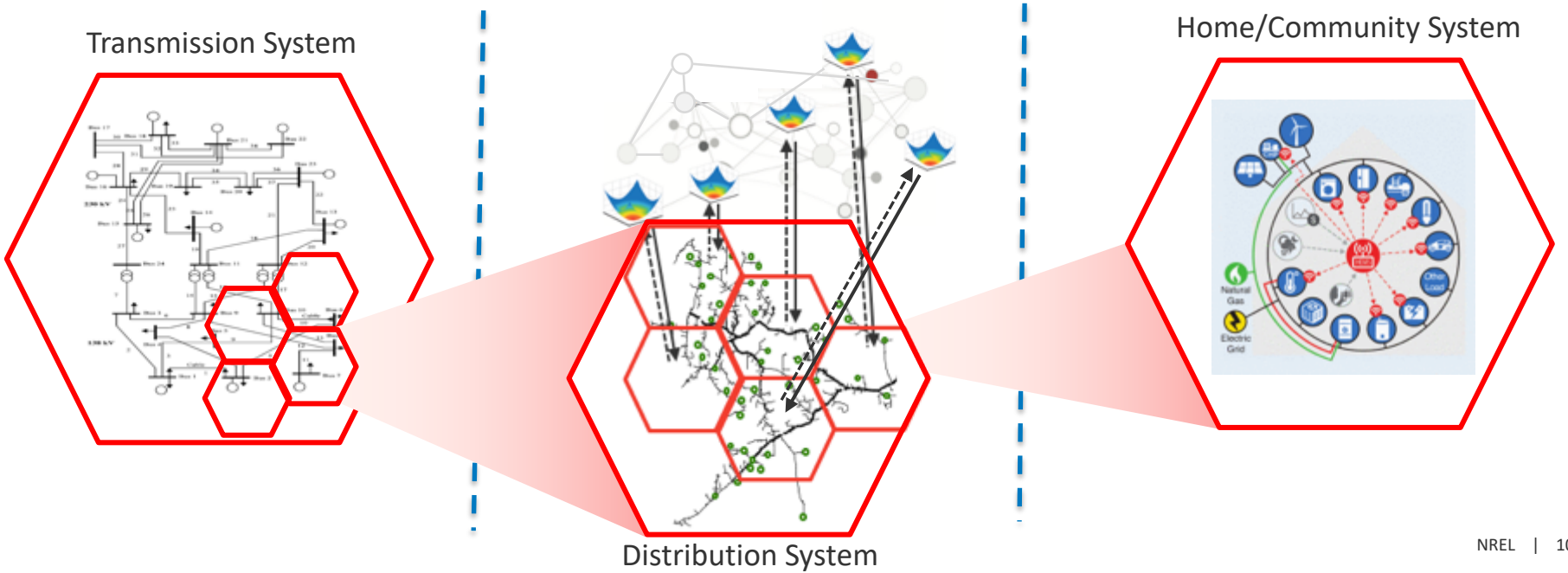
- **Bridge the gap between control theory and optimization theory** and **propose a unified theoretical approach** that builds on contemporary advances in control, optimization, and parallel computing
- Develop distributed optimization **algorithms that can run in real-time** (1s) across full system
- **Ensure a computationally affordable, optimal, resilient, and reliable distributed operation** with the objective to enable flexible operation and maintain stability and optimality
- **Validate the results in relevant real-world applications**



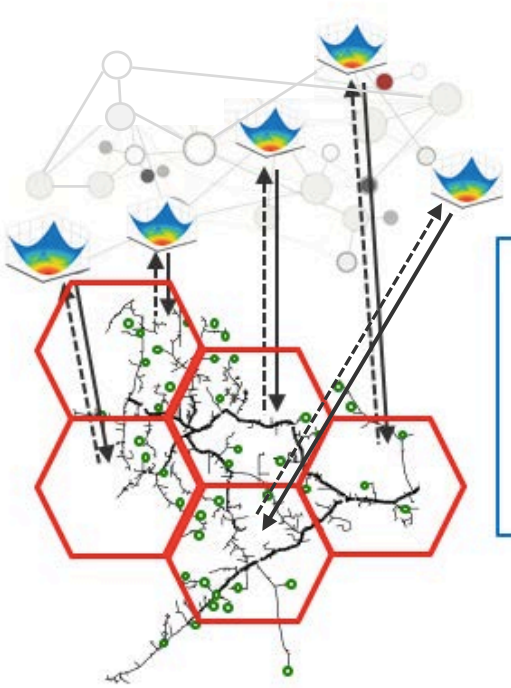
Formulating new math to address challenges

Challenges that are being addressed:

1. **Distributed** – Needs to be fast enough to operate in real-time (On-line)
2. **Scalable** – Needs to be able to control millions of devices (Hierarchical)
3. **Data Aware** – Make best use of time-varying asynchronous measurements



Distributed Control and Optimization



Real-time optimization with missing model parameters

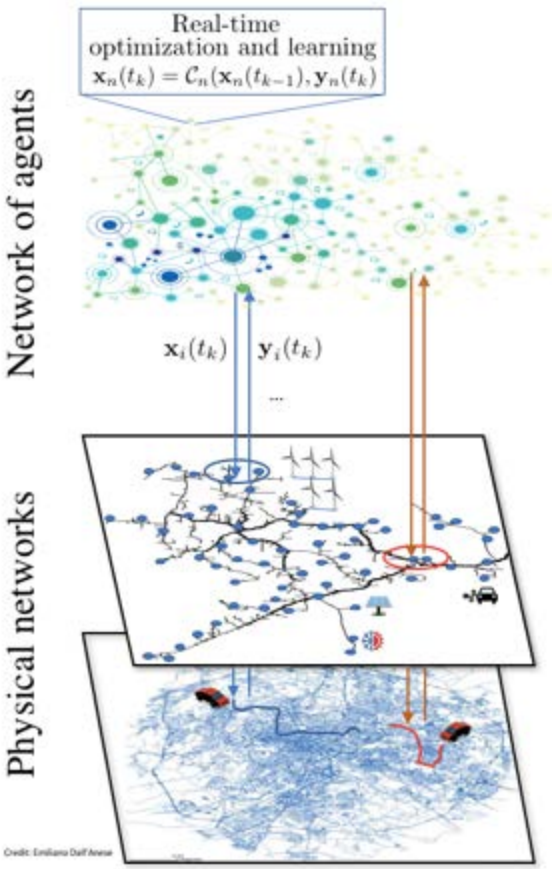
- *"Online Optimization with Feedback",* A. Bernstein, E. Dall'Anese, and A. Simonetto accepted to ***IEEE Transactions on Signal Processing***
- *"Online Optimization as a Feedback Controller: Stability and Tracking",* M. Colombino, E. Dall'Anese and A. Bernstein, submitted to ***IEEE Transactions on Control of Network Systems***

$$\min_{\mathbf{x},\mathbf{p}_i,\mathbf{q}_i} \; f_{net}(\mathbf{x}) + \sum_{DERs} f_i(\mathbf{p}_i,\mathbf{q}_i)$$
$$\text{subject to} \quad \mathbf{p}_i,\mathbf{q}_i \in \mathcal{Y}_i \;\forall i,$$
$$\mathbf{h}_i(\mathbf{p}_i,\mathbf{q}_i) = \mathbf{0} \;\forall i,$$
$$\mathbf{g}_i(\mathbf{p}_i,\mathbf{q}_i) \leq \mathbf{0} \;\forall i,$$
$$\mathbf{h}_{net}(\mathbf{x},\mathbf{p},\mathbf{q}) = \mathbf{0}$$
$$\mathbf{g}_{net}(\mathbf{x},\mathbf{p},\mathbf{q}) \leq \mathbf{0}$$

Unique Impactful Results

- Unique results in terms of convergence/stability of the algorithms for **real-time/ closed-loop optimization** algorithms that utilize measurements
- New mathematical framework for driving dynamic system to **optimal time-varying solutions**

Integration of Data Analytics - Formulating new math (ADMM-RL)



Combining Distributed Optimization and Learning (data-driven optimization)

- *"Distributed Reinforcement Learning with ADMM-RL",* Peter Graf, Jennifer Annoni, Christopher Bay, Dave Biagioni, Devon Sigler, Monte Lunacek, Wesley Jones submitted to the ***ACC Conference***

Alternating Direction Method of Multipliers (ADMM)

Decomposition-coordination procedure in which the solutions to small local subproblems (optimization) are coordinated to find a solution to a large global problem.

$$\begin{aligned} &\text{minimize } f(x) + g(z) \\ &\text{s.t. } Ax + Bz = c \end{aligned}$$

$$\begin{aligned} &\text{minimize } \sum_i f_i(x_i) \\ &\text{s.t. } x_i = z. \end{aligned}$$

+

Reinforcement Learning (RL)

Learner discovers what action yields maximum reward.

$$\begin{aligned} x_i^{k+1} &= \underset{x_{p(i)}}{\text{argmin-RL(n)}}\, f_i(x_i) + y_k^{k,T}(x_i - \bar{x}^k) + \\ &\quad \frac{\rho}{2}\|x_i - \bar{x}^k\|^2 \\ y^{k+1} &= y^k + \rho(x_i^{k+1} - \bar{x}^{k+1}), \end{aligned}$$

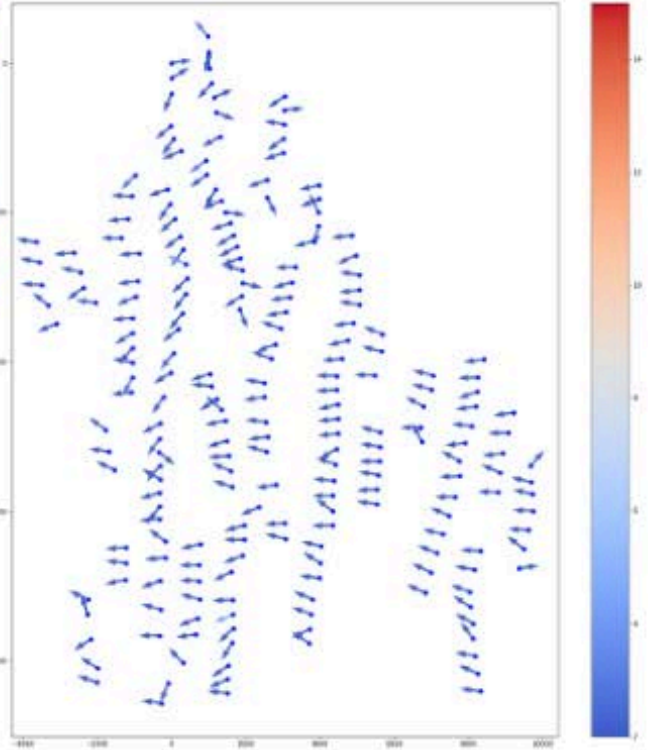
This Paper introduced a ADMM-RL controller to train wind turbines and water heater controls

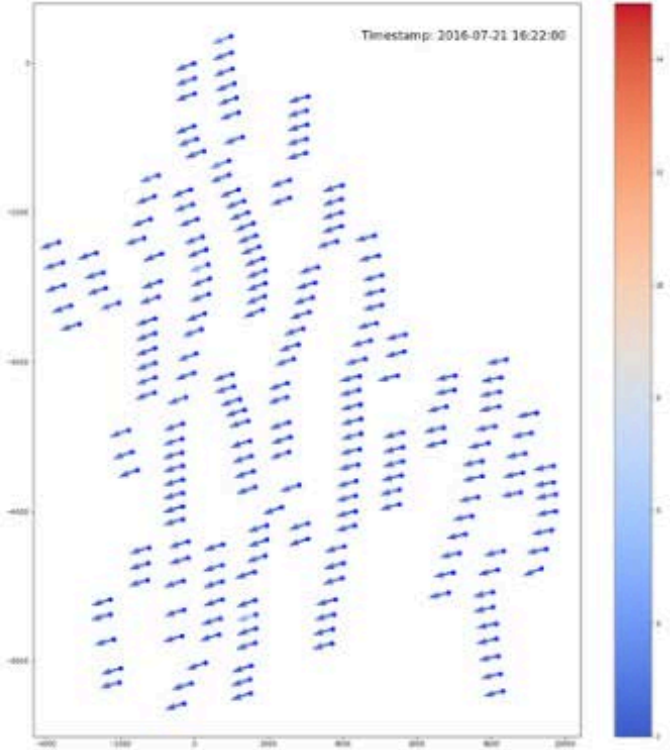
Application – Distributed Control of Wind Farms

Typical Wind Farm Control

(Each turbine moves based on local wind measurements)







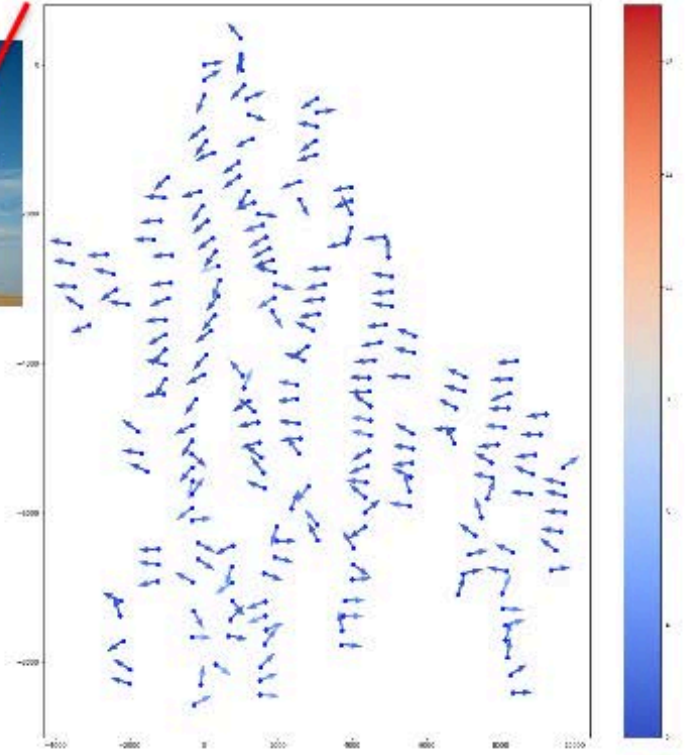
https://www.youtube.com/watch?v=nYV_LH46ZOU

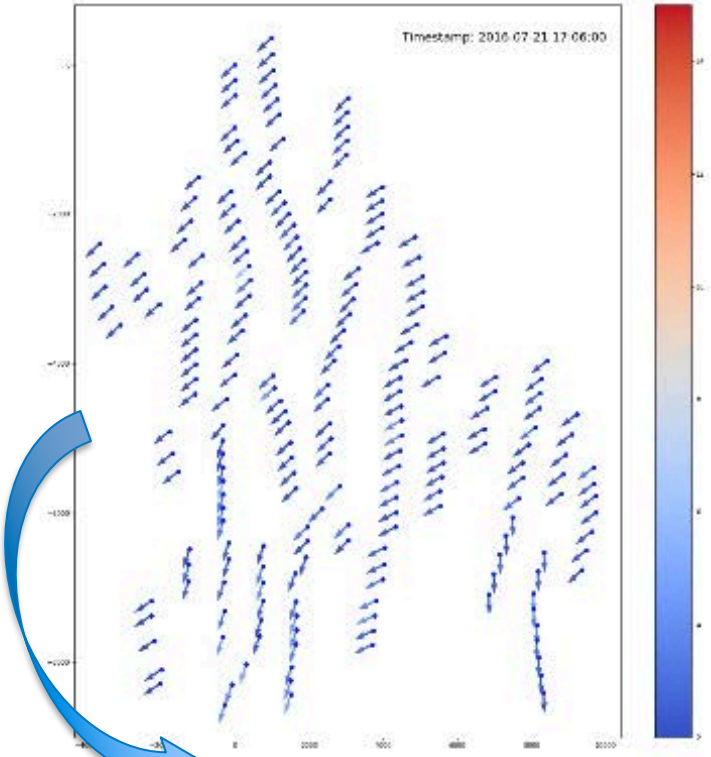
Application – Distributed Control of Wind Farms

Typical Wind Farm Control

(Each turbine moves based on local wind measurements)







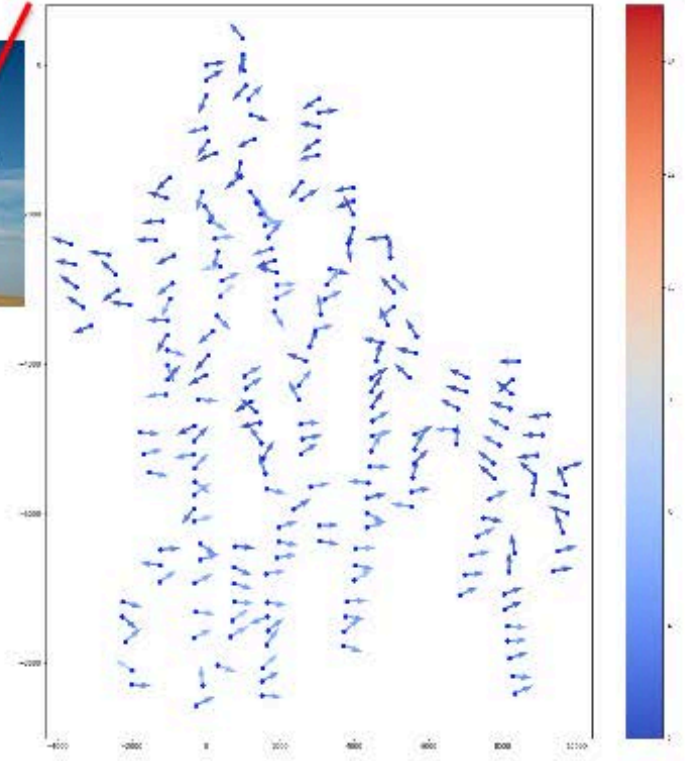
Wind Direction Shift

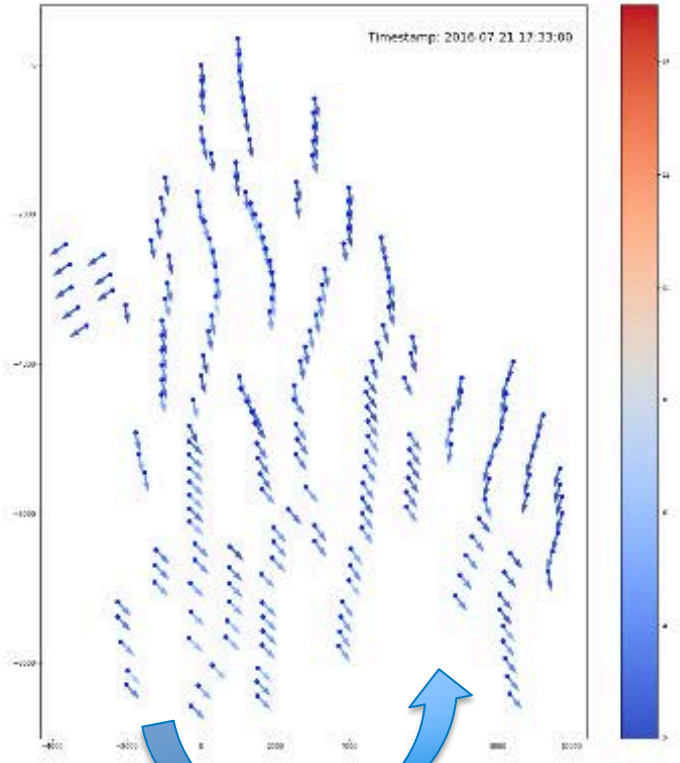
Application – Distributed Control of Wind Farms

Typical Wind Farm Control

(Each turbine moves based on local wind measurements)







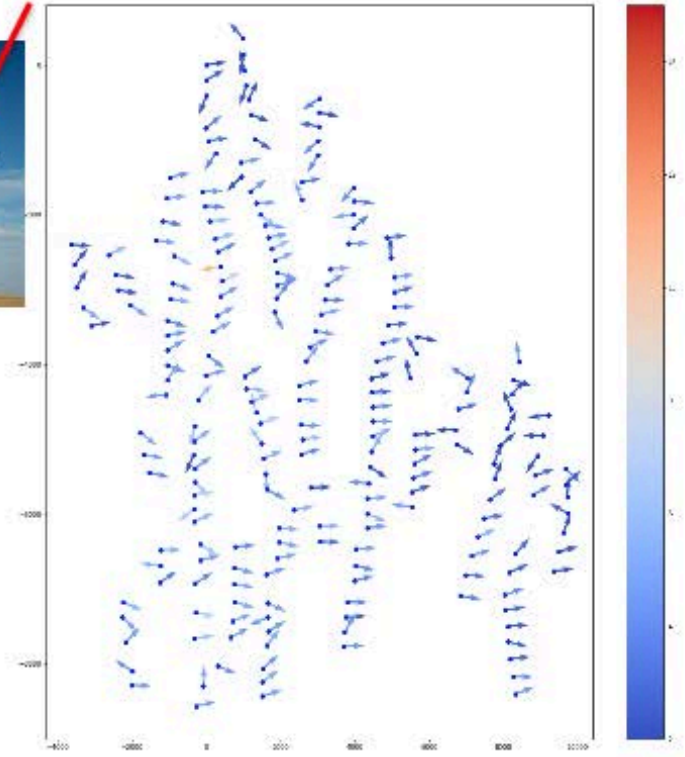
Wind Direction Shift

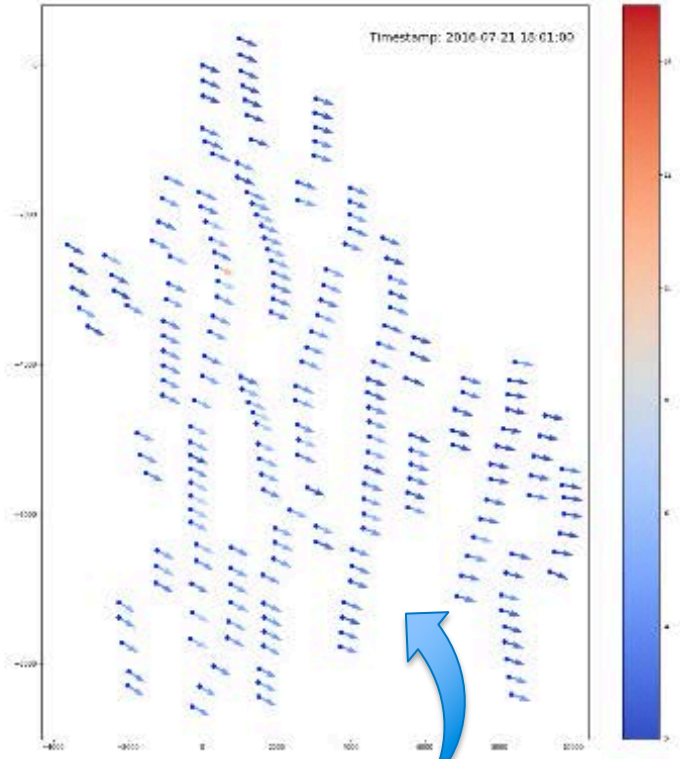
Application – Distributed Control of Wind Farms

Typical Wind Farm Control

(Each turbine moves based on local wind measurements)







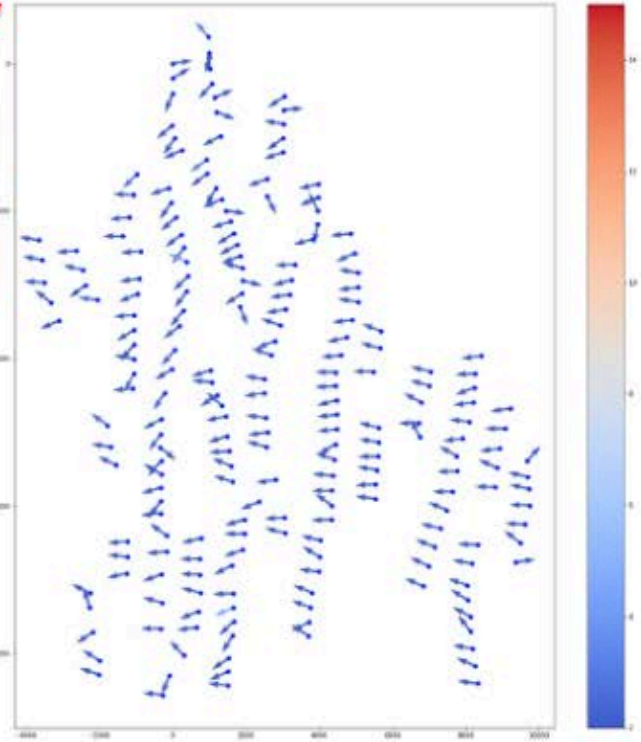
Wind Direction Shift

Application – Distributed Control of Wind Farms

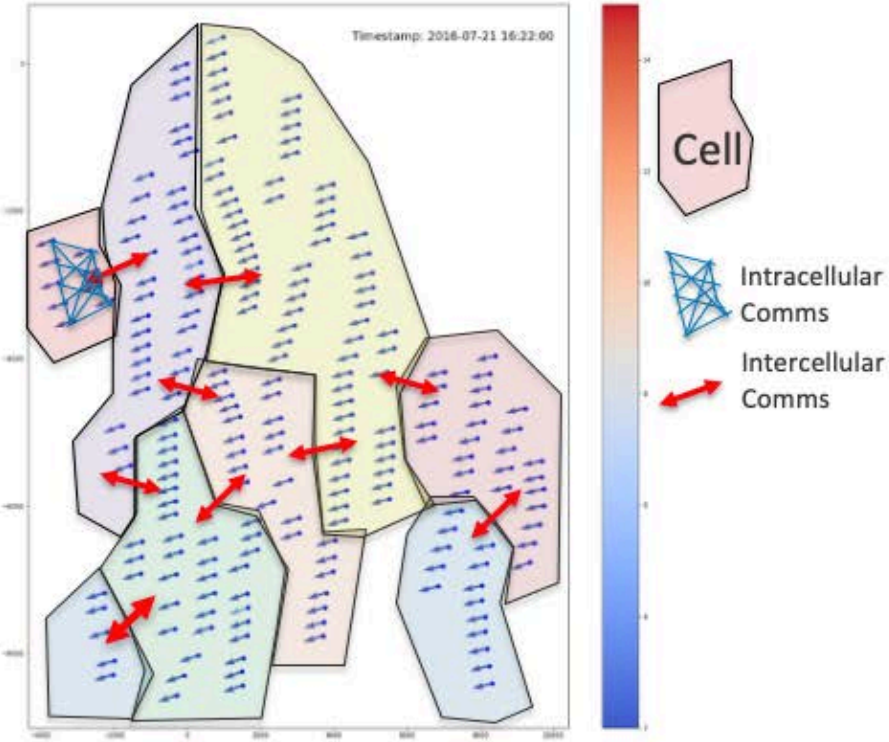
Typical Wind Farm Control

(Each turbine moves based on local wind measurements)





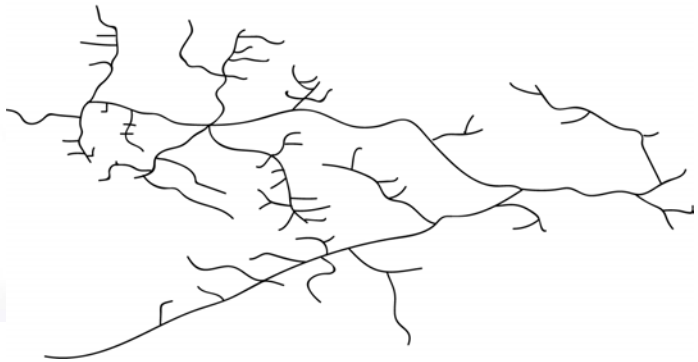
Distributed Wind Farm Control



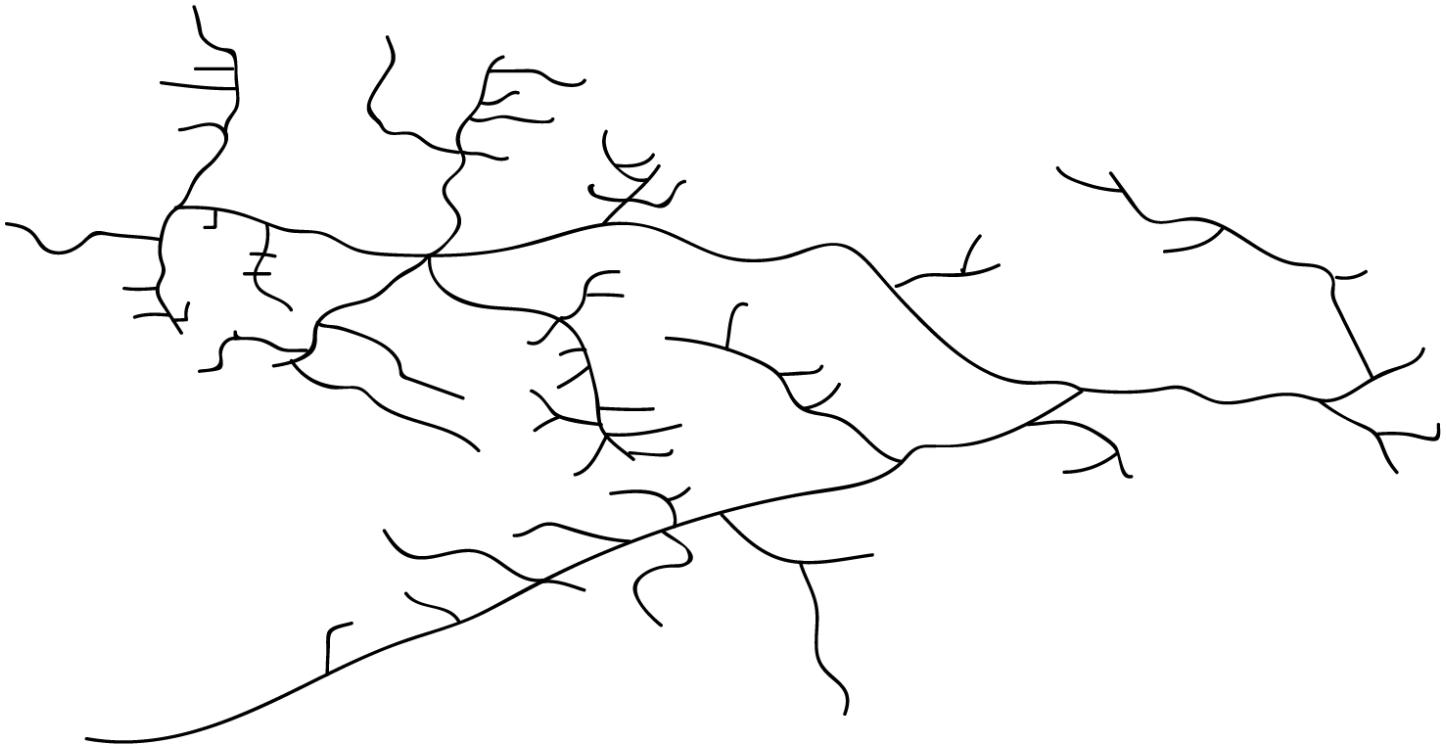
- Solution from Central Control of **13.75min** to Distributed Control of **2s**
- **Allowing ~2% more energy production annually**

Let’s look a little closer – a single distribution circuit



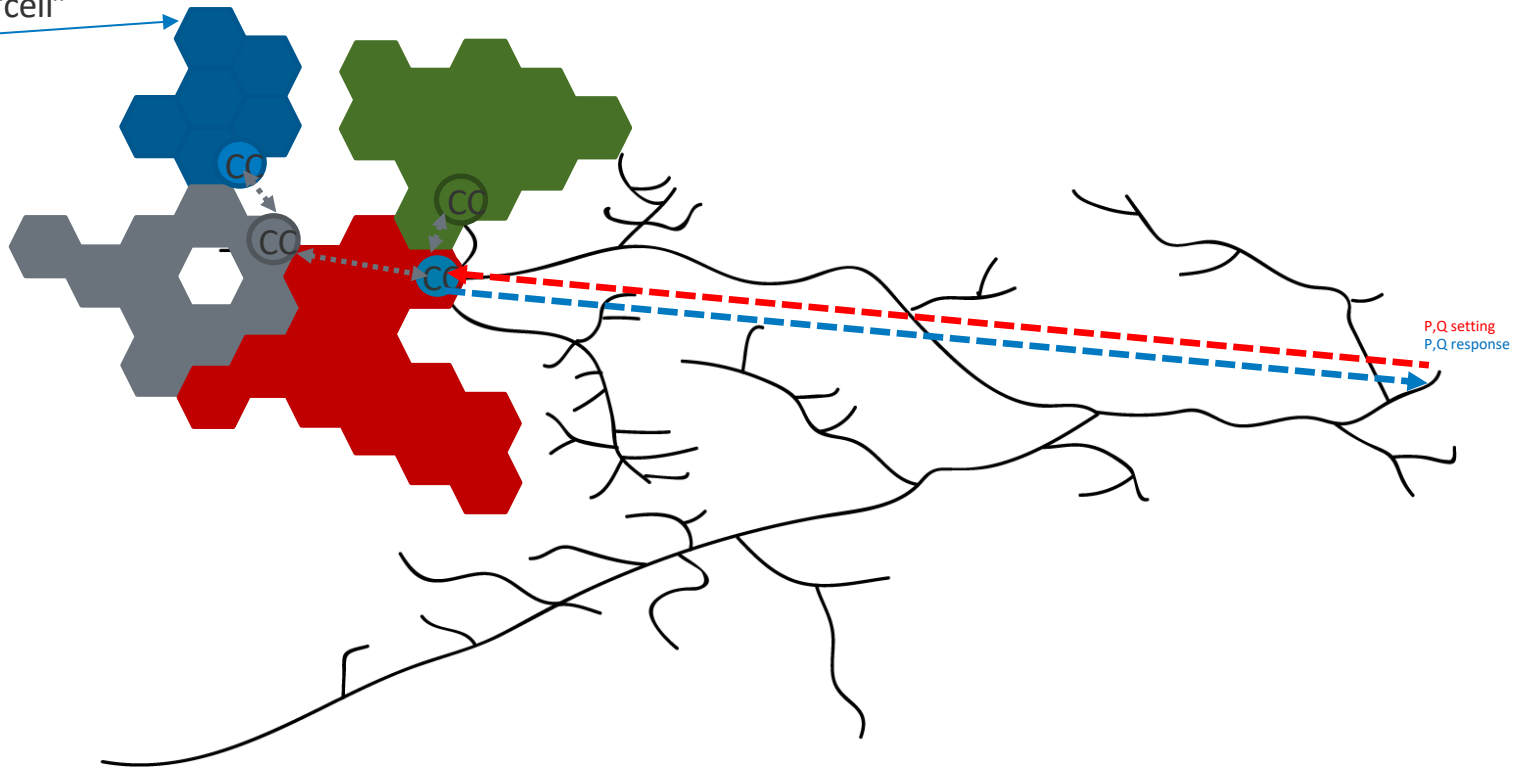


Complex system simulation with new optimization and controls

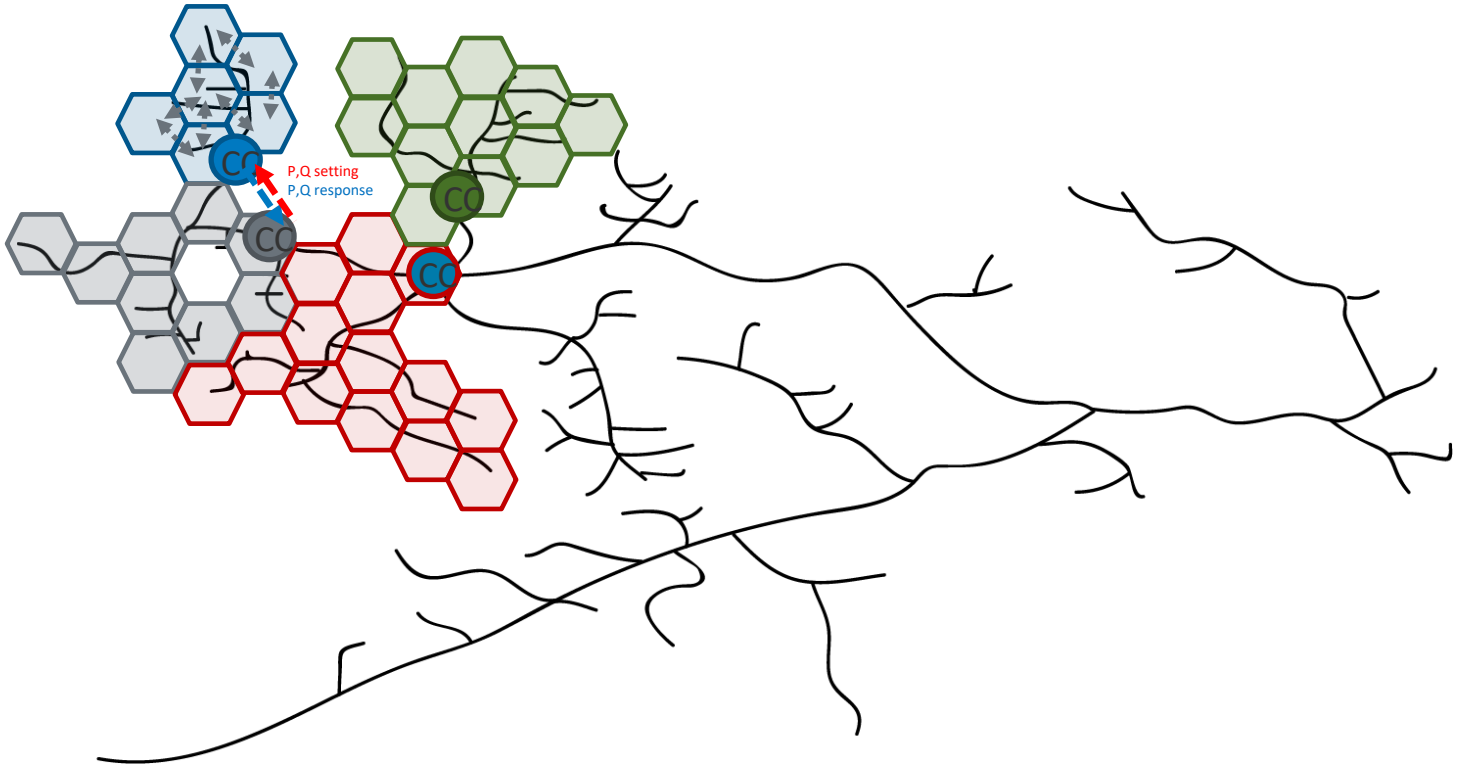


Complex system simulation with new optimization and controls

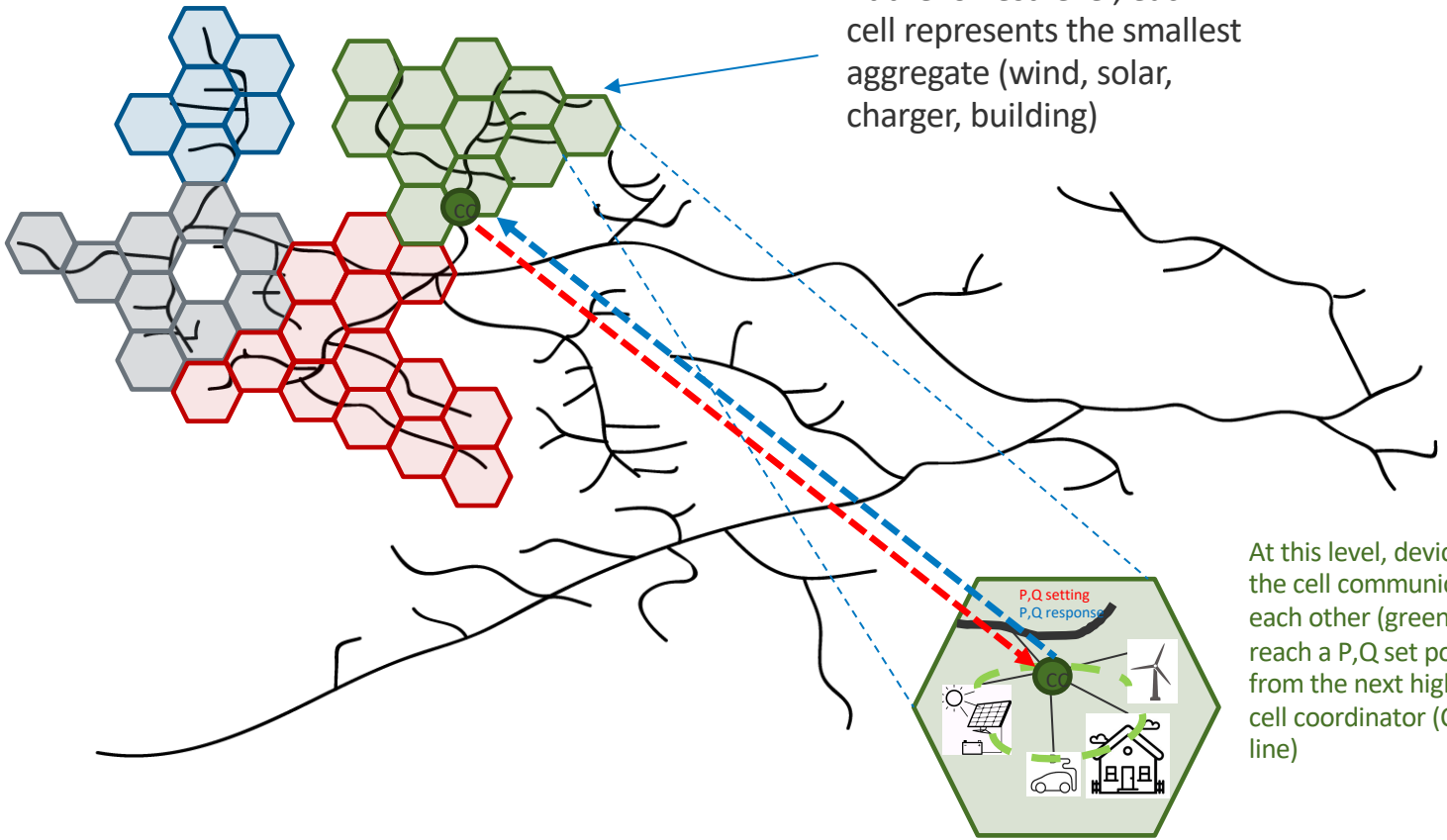
Color coding represent the next higher “cell”



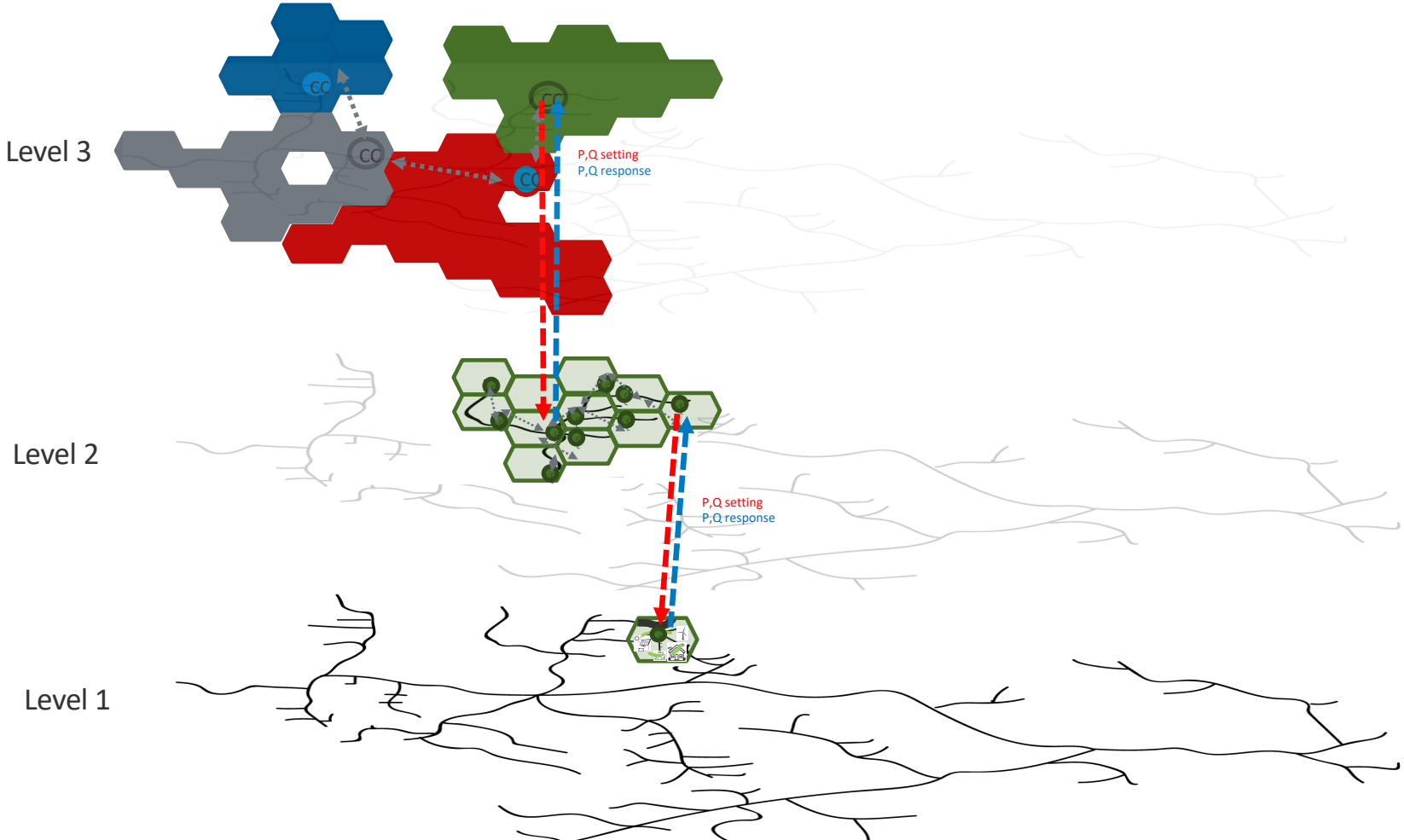
Complex system simulation with new optimization and controls



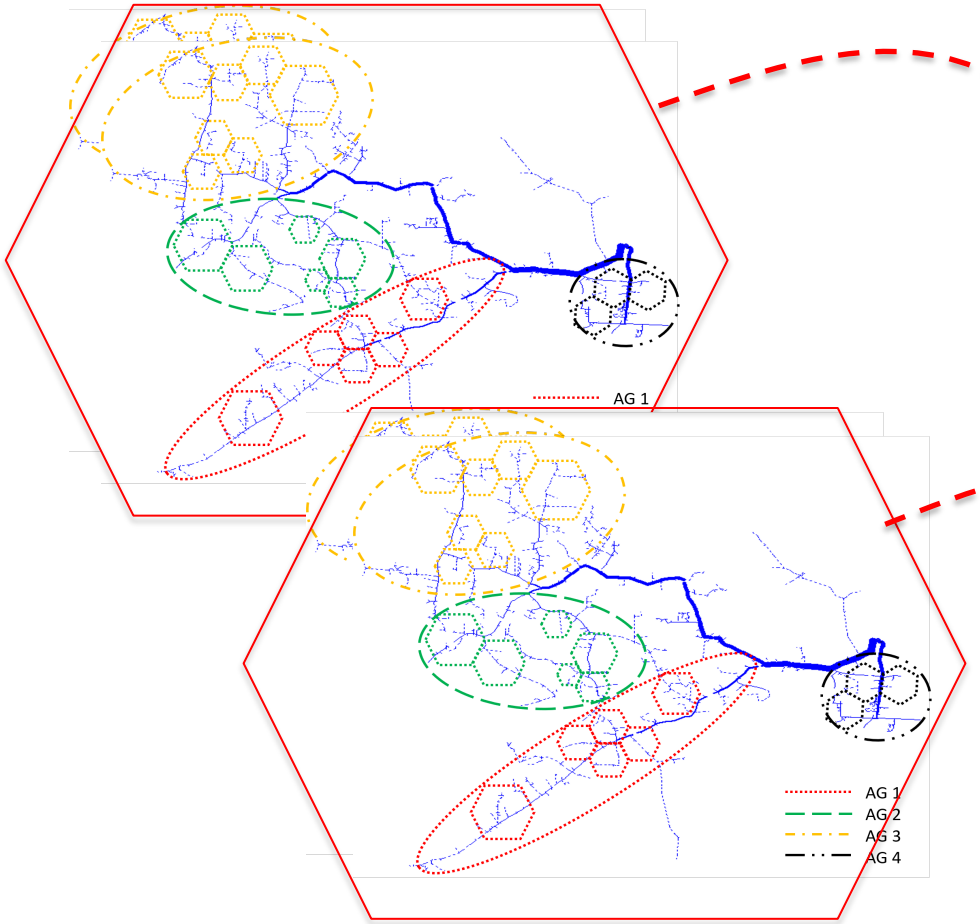
Complex system simulation with new optimization and controls

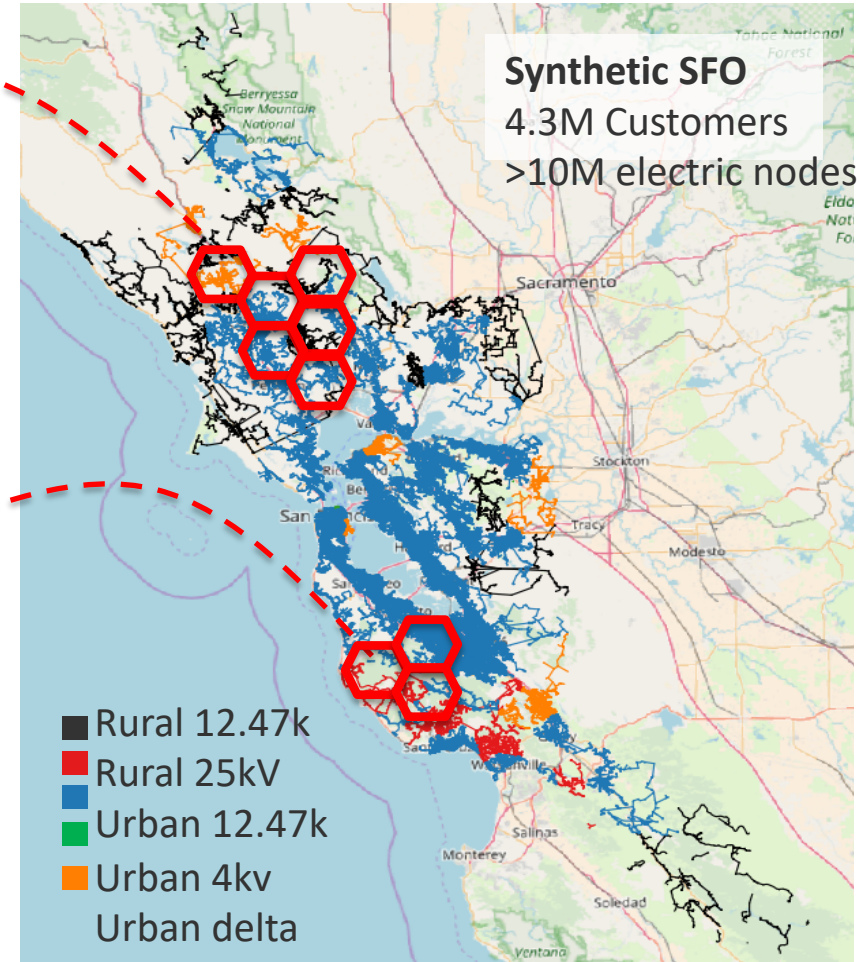


In 3D


Level 3
Level 2
Level 1
CC
CC
CC
P,Q setting
P,Q response
P,Q setting
P,Q response

Moving Back to the Metropolitan Scale





All that Simulation was nice, but can you show me it really works?




Energy Systems Integration Facility (ESIF)







Shortening the time between innovation and practice

ESIF Unique Capabilities

- Multiple parallel AC and DC experimental busses (MW power level) with grid simulation and loads
- Flexible interconnection points for electricity, thermal, and fuels
- Medium voltage (15kV) microgrid test bed
- Virtual utility operations center and visualization rooms
- Smart grid testing lab for advanced communications and control
- Interconnectivity to external field sites for data feeds and model validation
- Petascale HPC and data mgmt system in showcase energy efficient data center
- **MW-scale Power hardware-in-the-loop (PHIL) simulation capability to test grid scenarios with high penetrations of clean energy technologies**

ARPA-E NODES: Large-Scale PHIL Experiment

The largest ever number of connection points in a single PHIL experiment!

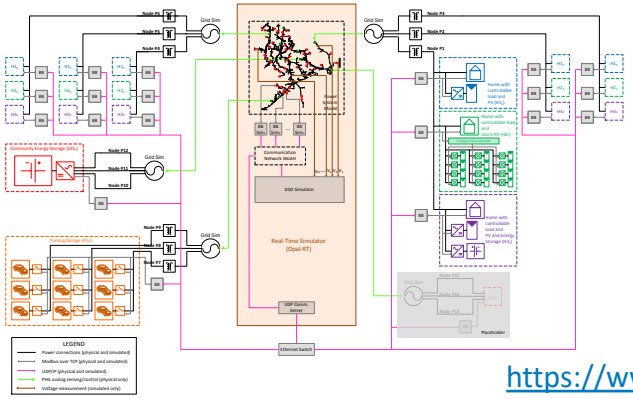












Network Optimized Distributed Energy Systems (NODES)

arpa·e
CHANGING WHAT'S POSSIBLE

https://www.youtube.com/watch?v=In4HtG6XypU

Let’s Look to the Future

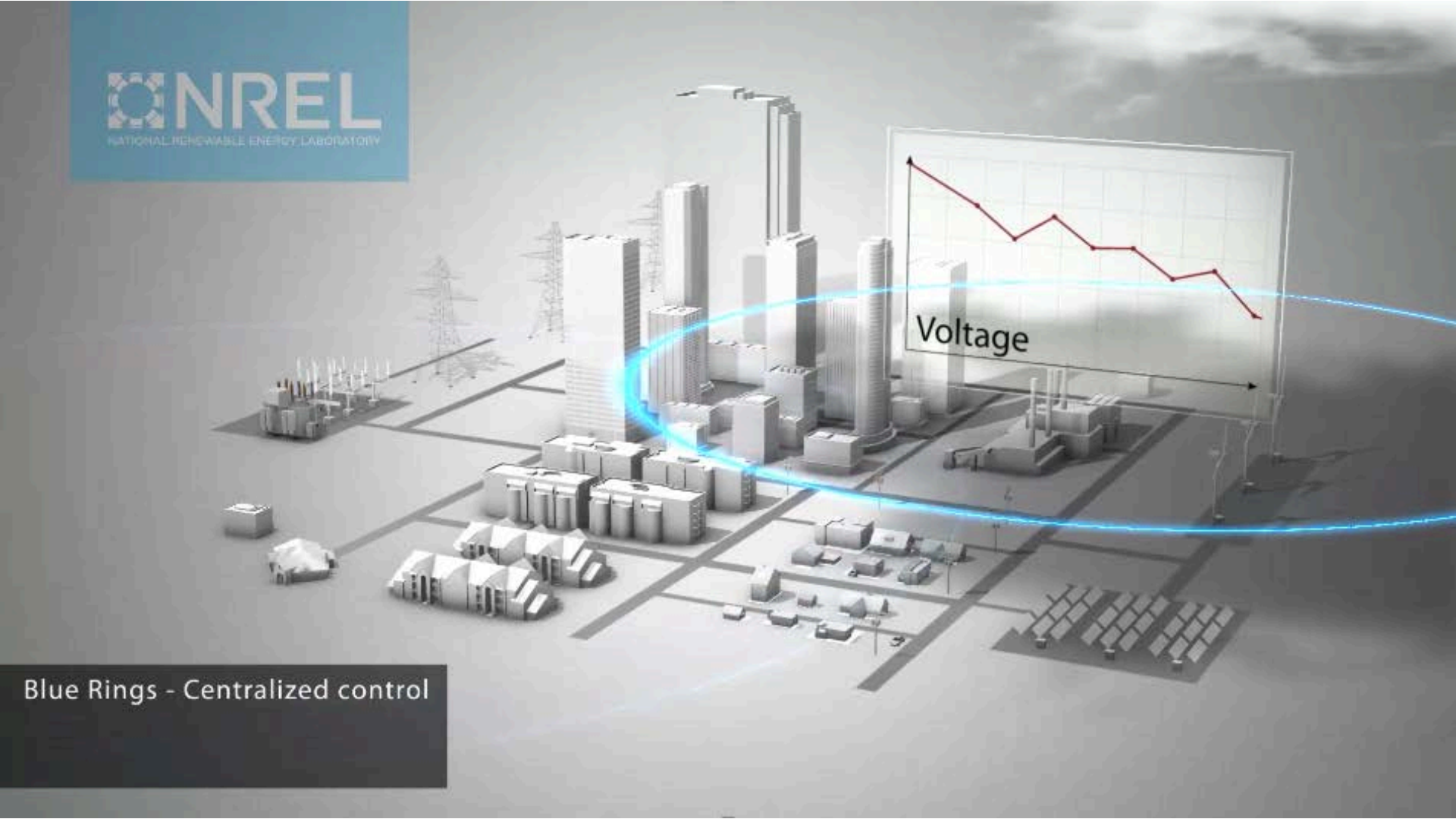


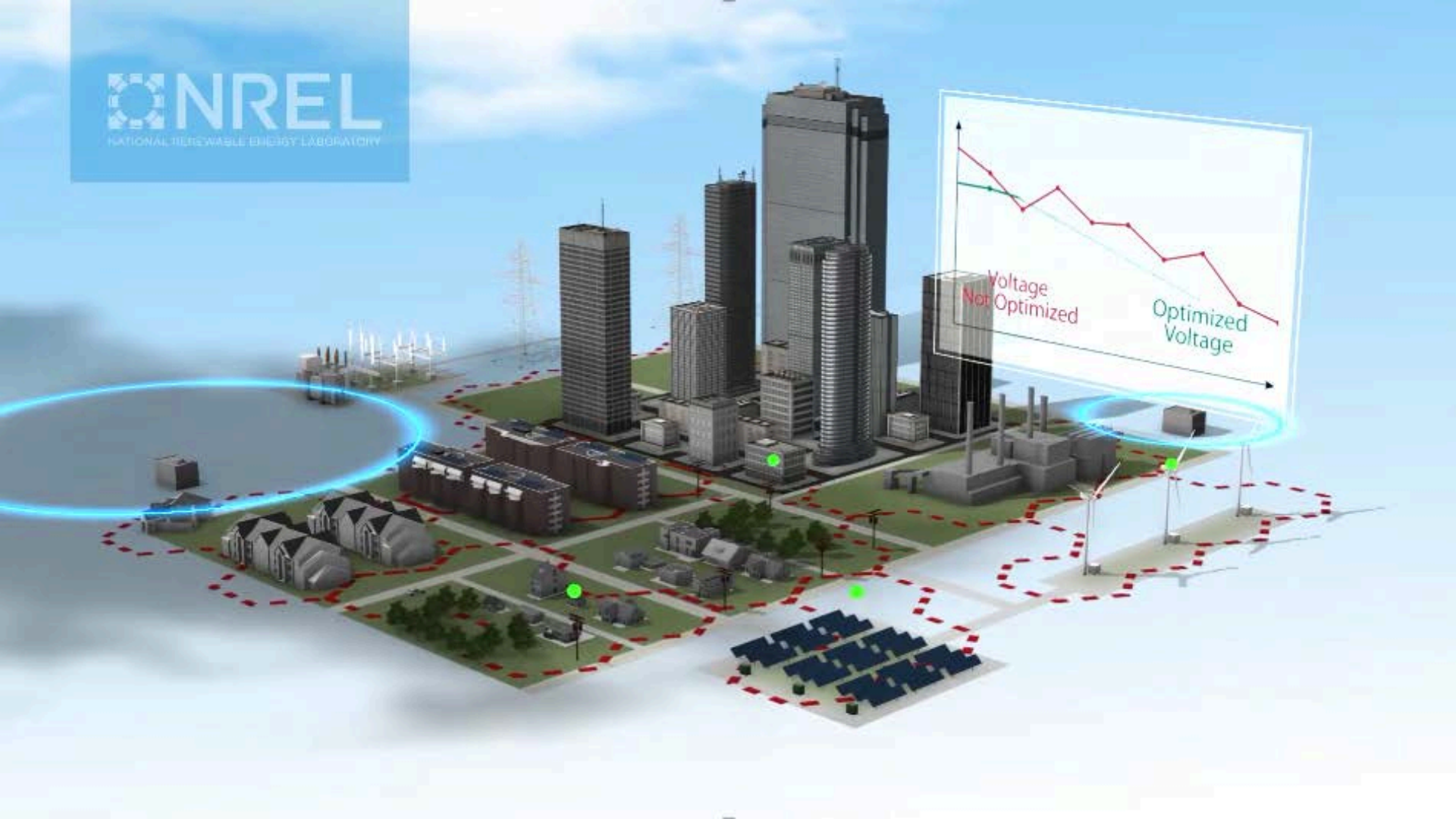
NREL
NATIONAL RENEWABLE ENERGY LABORATORY

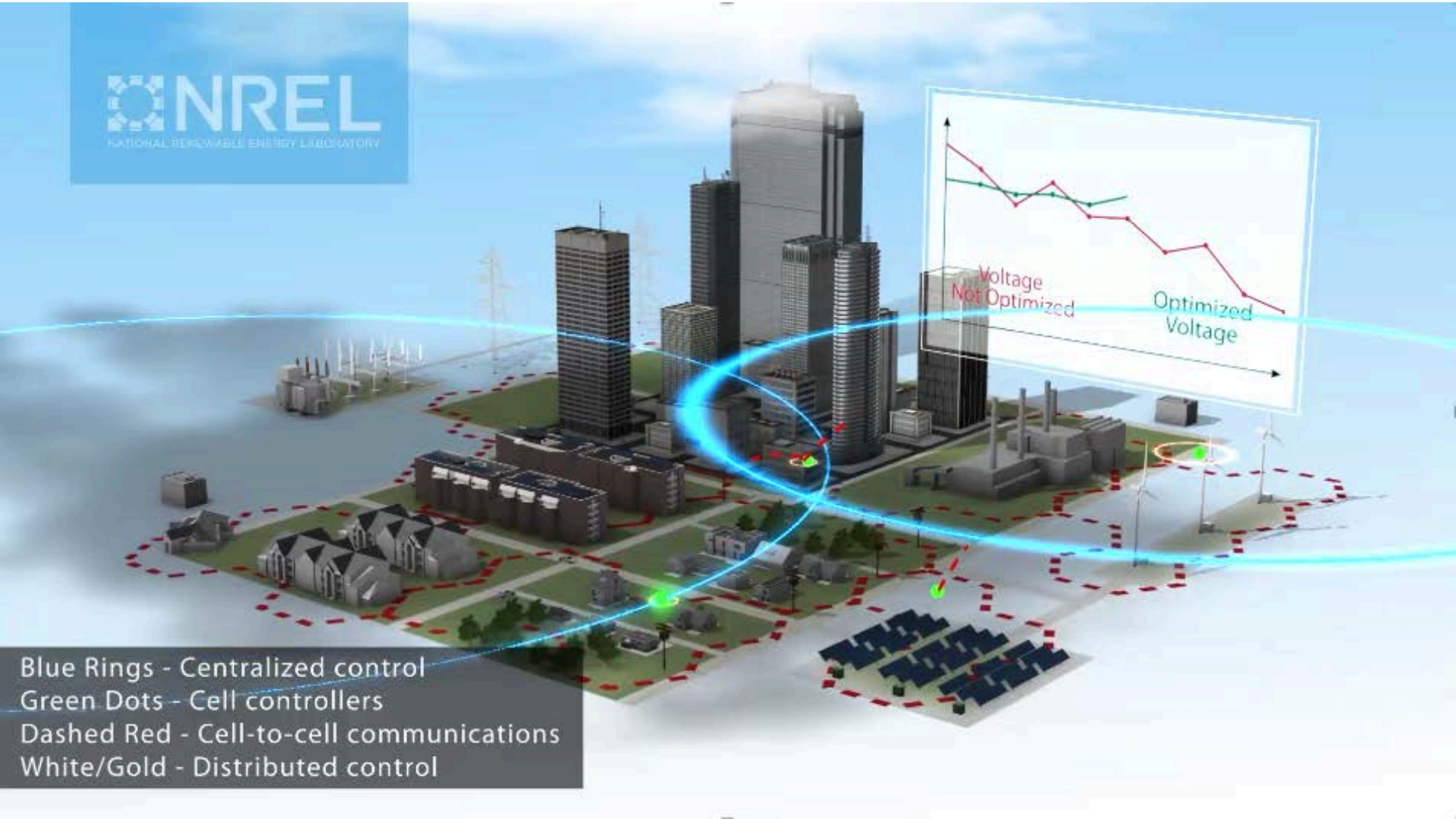
Autonomous Energy Grids

NREL is a national laboratory of the U.S. Department of Energy,
Office of Energy Efficiency and Renewable Energy, operated by the Alliance for Sustainable Energy, LLC.


NREL
NATIONAL RENEWABLE ENERGY LABORATORY
Voltage


NREL
NATIONAL RENEWABLE ENERGY LABORATORY
Voltage
Blue Rings - Centralized control


NREL
NATIONAL RENEWABLE ENERGY LABORATORY
Voltage
Not Optimized
Optimized
Voltage


NREL
NATIONAL RENEWABLE ENERGY LABORATORY
Voltage
Not Optimized
Optimized
Voltage
Blue Rings - Centralized control
Green Dots - Cell controllers
Dashed Red - Cell-to-cell communications
White/Gold - Distributed control


NREL
NATIONAL RENEWABLE ENERGY LABORATORY
Voltage
Not Optimized
Optimized
Voltage
Blue Rings - Centralized control
Green Dots - Cell controllers
Dashed Red - Cell-to-cell communications
White/Gold - Distributed control

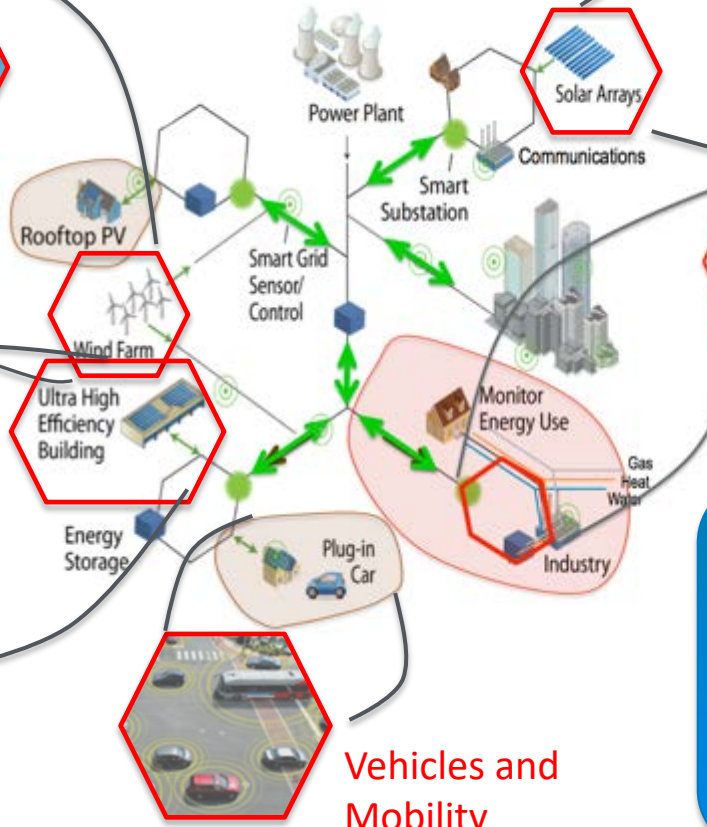
Transforming ENERGY through Autonomous Energy Systems

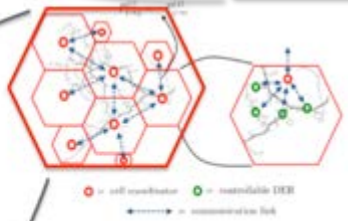
Advanced Wind Plants



Advanced Solar Plants







Autonomous Energy Grids



Grid Interactive Efficient Buildings

Vehicles and Mobility

- Integration of all energy sources
- Scalable, distributed control of millions of devices
- Real-time optimization
- Able to integrate asynchronous data and communications

Thank you

www.nrel.gov/grid/autonomous-energy.html