bcuc
British Columbia
Utilities Commission

Suite 410, 900 Howe Street
Vancouver, BC Canada V6Z 2N3
bcuc.com

P: 604.660.4700
TF: 1.800.663.1385
F: 604.660.1102

ORDER NUMBER
R-34-22A1

IN THE MATTER OF
the *Utilities Commission Act*, RSBC 1996, Chapter 473

and

British Columbia Hydro and Power Authority
Mandatory Reliability Standards Assessment Report No. 15
Addressing Reliability Standards for Adoption in British Columbia

BEFORE:
C. M. Brewer, Panel Chair
W. M. Everett, KC, Commissioner
A. K. Fung, KC, Commissioner

on October 28, 2022

ORDER

WHEREAS:

A. On April 29, 2022, pursuant to section 125.2(3) of the *Utilities Commission Act* (UCA), British Columbia Hydro and Power Authority (BC Hydro) submitted to the British Columbia Utilities Commission (BCUC) Mandatory Reliability Standards (MRS) Assessment Report No. 15 (Report) assessing 14 revised reliability standards (Revised Standards) and five reliability standards considered for retirement (Retired Standards);

B. In the Report, BC Hydro recommends that with the exception of Revised Standard PRC-006-5 referred to in recital C below, 13 of the 14 Revised Standards are suitable for adoption in British Columbia (BC) at this time as they will preserve or enhance the reliability of the bulk electric system (BES), and serve the public interest and that the five Retired Standards be retired;

C. In the Report, BC Hydro states that all the requirements of the Revised Standard PRC-006-5 Automatic Underfrequency Load Shedding (Revised Standard PRC-006-5) are either dependent on and/or require actions solely by the Planning Coordinator (PC) and should be held in abeyance and be of no force or effect in BC until the role of the PC as it pertains to BC is resolved;

D. Further, BC Hydro states that the Report does not include the adoption or retirement of defined terms from the North American Electric Reliability Corporation (NERC) Glossary of Terms (NERC Glossary) dated June 28, 2021, as the NERC Glossary contains no new revised or retired terms related to the reliability standards adopted in BC;

E. By Order R-22-22 dated July 8, 2022, the BCUC established a regulatory timetable and a written comment process for the review of the Report and directed BC Hydro to make the Report available on its external website and to notify all Entities registered in the British Columbia Mandatory Standards Program of the review process;

F. On August 8, 2022, FortisBC Inc. (FBC) submitted a letter of comment and on August 15, 2022, BC Hydro filed its response to FBC's letter of comment;

G. By Order R-31-22 dated September 20, 2022, the BCUC amended the regulatory timetable which included one round of information requests (IRs);

H. On September 29, 2022, BC Hydro and FBC submitted their responses to BCUC IR No. 1;

I. The BCUC did not review the recoverability of the estimated costs to adopt the Revised Standards;

J. Pursuant to section 125.2(6) of the UCA, the BCUC must adopt the reliability standards addressed in the report if the BCUC considers that the reliability standards are required to maintain or achieve consistency in BC with other jurisdictions that have adopted the reliability standards;

K. The BCUC has reviewed and considered the Report, the Revised Standards and the Retired Standards assessed therein, comments received from Entities and the responses to IRs and determines that adoption of the recommendations in the Report is warranted with an amended consolidated BC-specific implementation plan for reliability standards EOP-011-2, IRO-010-4 and TOP-003-5; and

L. Although not assessed by BC Hydro, the BCUC finds that the compliance provisions of the reliability standards (Compliance Provisions) should be adopted to maintain compliance monitoring consistency with other jurisdictions that have adopted the reliability standards with the Compliance Provisions. The BCUC also considers it appropriate to provide effective dates for BC Entities to come into compliance with the Revised Standards and Retired Standards adopted in this Order.

NOW THEREFORE pursuant to sections 125.2(3) and 125.2(6) of the UCA, and for the reasons attached as Appendix A to this order, the BCUC orders as follows:

1. With the exception of Revised Standard PRC-006-5, thirteen (13) of the fourteen (14) Revised Standards assessed in the Report are adopted with effective dates as identified in Table 1 of Attachment A to this Order. Each standard to be superseded by a Revised Standard adopted in this Order shall remain in effect until the effective date of the Revised Standard superseding it.

2. The five (5) Retired Standards assessed in the Report are retired with effective dates as identified in Table 1 of Attachment A to this Order.

3. Revised Standard PRC-006-5 assessed in the Report is held in abeyance and is of no force or effect in BC until the role of the Planning Coordinator as it pertains to BC is resolved.

4. All reliability standards listed in Attachment B to this Order are effective in BC as of the dates shown. The effective dates for the reliability standards listed in Attachment B supersede the effective dates that were included in any similar list appended to any previous order of the BCUC.

5. Individual requirements within reliability standards that incorporate by reference reliability standards that have not been adopted by the BCUC are of no force and effect in BC, and individual requirements or sub-requirements within reliability standards, which the BCUC has adopted but for which the BCUC has not determined an effective date, are of no force and effect in BC.

6. Defined terms set out in the reliability standards bear the same meanings as those set out in the NERC Glossary dated June 28, 2021. Other terms in the NERC Glossary, which do not include a United States Federal Energy Regulatory Commission (FERC) approval date on or before November 30, 2021, are of no force or effect in BC.

7. All defined terms listed in Attachment C to this Order are in effect in BC as of the effective dates indicated.

8. The Compliance Provisions as defined in the Rules of Procedure for Reliability Standards in British Columbia that accompany each of the adopted reliability standards, are approved in the form directed by the BCUC and as amended from time to time.

9. The BC-specific Implementation Plan for CIP-005-7, CIP-010-3 and CIP-013-2 is adopted and the standards are effective on the dates in the respective standards as set out in Attachment E to this Order.

10. The BC-specific Implementation Plan for EOP-011-2, IRO-010-4 and TOP-003-5 is adopted with revisions and the standards are effective on the dates in the respective standards in Attachment E to this Order.

11. BC Hydro is directed to include the revised standard FAC-001-3 Errata for review in BCUC's review of Assessment Report No. 16 .

12. As BC Hydro's assessment of the FAC-001-3 Errata was omitted from Assessment Report No. 15, BC Hydro must file a quarterly report listing all the new, revised and retired NERC and Western Electricity Coordinating Council (WECC) reliability standards and Glossary terms approved by the FERC, along with the effective dates of the approval. The assessment quarters must be aligned with the Assessment Report Period December 1 to November 30 of the following year. Each quarterly report must be cumulative and must include all new, revised and retired standards listed in prior quarterly reports for the current Assessment Report Period. The quarterly assessment report must be filed with the BCUC by the end of the calendar month following the assessment quarter. The first quarterly filing is due by March 31, 2023, for the Assessment Report Period December 1, 2022 through November 30, 2023. The report must include, at a minimum, the following information:

    1) NERC or WECC Reliability Standard number and title and FERC approval effective date; and

    2) BC Hydro's preliminary assessment of:

        i. any adverse impact of the reliability standard on the reliability of electricity transmission in BC if the reliability standard were adopted;

        ii. the suitability of the reliability standard for BC; and

        iii. whether a particular reliability standard is sufficiently critical to reliability that it warrants immediate implementation.

13. With the exception of Revised Standard PRC-006-5, the Revised Standards in their written form are adopted as set out in Attachment E to this Order.

14. The reliability standards and their associated BC-specific implementation plans adopted in BC by the BCUC are posted on the WECC website with a link from the BCUC website.

15. Entities subject to Mandatory Reliability Standards adopted in BC must report to the BCUC and may, on a voluntary basis, report to NERC or to FERC.

DATED at the City of Vancouver, in the Province of British Columbia, this 3rd day of November 2022.

BY ORDER

Original signed by:

C. M. Brewer
Commissioner

Attachments

British Columbia Hydro and Power Authority
Mandatory Reliability Standards Assessment Report No. 15
Addressing Reliability Standards for Adoption in British Columbia

REASONS FOR DECISION

1.0 Application

On April 29, 2022, pursuant to section 125.2(3) of the *Utilities Commission Act* (UCA), British Columbia Hydro and Power Authority (BC Hydro) submitted to the British Columbia Utilities Commission (BCUC) Mandatory Reliability Standards (MRS) Assessment Report No. 15 (Report) assessing 14 revised reliability standards (Revised Standards) and five reliability standards considered for retirement (Retired Standards).

1.1 Regulatory and Legislative Process

By Order R-22-22 dated July 8, 2022, the BCUC established a regulatory timetable and a written comment process for the review of the Report and directed BC Hydro to make the report available on its external website and to notify all Entities registered in the British Columbia MRS Program of the review process.

On August 8, 2022, FortisBC Inc. (FBC) submitted a letter of comment and on August 15, 2022, BC Hydro filed its response to FBC's letter of comment.

By Order R-31-22 dated September 20, 2022, the BCUC amended the regulatory timetable which included one round of information requests (IR No. 1).

On September 29, 2022, BC Hydro and FBC submitted their responses to BCUC IR No. 1.

1.2 Regulatory Authority

In determining whether reliability standards should be adopted in BC, the Panel considers the following sections of the UCA which are summarized below:

Section 125.2(2)

For greater certainty, the BCUC has exclusive jurisdiction to determine whether a reliability standard is in the public interest and should be adopted in British Columbia.

Section 125.2(5)

If the BCUC receives a report under subsection (3), the BCUC must

(a) make the report available to the public in a reasonable manner, which may include by electronic means, and for a reasonable period of time, and

(b) consider any comments the BCUC receives in reply to the publication referred to in paragraph (a).

Section 125.2(6)

After complying with section 125.2(5), the BCUC, subject to section 125.2(7), must, by order, adopt the reliability standards addressed in the report if the BCUC considers that the reliability standards are required to maintain or achieve consistency in British Columbia with other jurisdictions that have adopted the reliability standards.

Section 125.2(7)

The BCUC is not required to adopt a reliability standard under section 125.2(6) if the BCUC determines, after a hearing, that the reliability standard is not in the public interest.

2.0 Reliability Standard PRC-006-5

On May 31, 2021, BC Hydro filed with the BCUC an assessment of the reliability standards that have dependency on and/or require actions solely by the Planning Coordinator (PC) (PC Assessment Report). By Order R-15-21 dated July 14, 2021, the BCUC established a proceeding to review the PC Assessment Report (PC Assessment Report Proceeding). Parties recommended that the BCUC suspend the PC Assessment Report Proceeding and establish a new proceeding to address issues related to the PC function in BC (PC Issues). By Order R-4-22 dated January 26, 2022, and after reviewing submissions from Registered Entities and the public, the BCUC adjourned the PC Assessment Report Proceeding and recommended the BCUC initiate a separate proceeding regarding the PC Issues identified.

By Order R-8-22 dated March 14, 2022, the BCUC established a separate proceeding to review the PC Issues in the currently adjourned PC Assessment Report Proceeding.

BC Hydro states that all of the requirements of the Revised Standard PRC-006-5 are either dependent on and/or require actions solely by entities registered for the Planning Coordinator function. BC Hydro further recommends that the Revised Standard PRC-006-5 be ordered by the BCUC to be held in abeyance and be of no force or effect in BC until the role of the PC as it pertains to BC is resolved.[1] BC Hydro states that once the PC function and footprints are defined, the Revised Standard PRC-006-5 and the reliability standards in the PC Assessment Report will go through the assessment process in BC.[2]

Panel Determination

The Panel notes that the PC Assessment Report Proceeding which reviews the reliability standards that have a dependency on and/or require actions solely by the PC is currently adjourned, pending the resolution of the PC Issues. Further, parties did not oppose BC Hydro's recommendation that Revised Standard PRC-006-5 be held in abeyance and be of no force or effect in BC for the time being.

Therefore, the Panel finds that it is appropriate that Revised Standard PRC-006-5 be held in abeyance and be of no force or effect in BC until the role of the PC as it pertains to BC is resolved.

[1] Exhibit B-1, p. 5.
[2] Exhibit B-1, p. 5.

3.0 Reliability Standard FAC-001-3 Facility Interconnection Requirements Errata

The North American Reliability Corporation (NERC) had revised reliability standard FAC-001-3 in 2021 on account of errata (FAC-001-3 Errata). The revised standard was approved by the United States Federal Energy Regulatory Commission (FERC) during the assessment period for the Report. This revised standard was not included in the Report because BC Hydro failed to correctly identify the revision.[3]

BC Hydro states that the errata changes are non-substantive in nature and that there is no perceived risk to the Bulk Electric System by maintaining the current FAC-001-3 standard in BC. BC Hydro further states that the revised standard FAC-001-3 Errata will be included in Assessment Report No. 16. BC Hydro will also perform a detailed comparison of such errata in future to avoid a similar situation as with FAC-001-3.[4]

Panel Determination

The Panel finds that the proposed errata changes are non-substantive in nature and that there is no perceived risk to the Bulk Electric System in not adopting the FAC-001-3 Errata in BC at this time. However, the Panel directs BC Hydro to include the revised standard FAC-001-3 Errata in Assessment Report No. 16 for review by the BCUC at that time.

Given that BC Hydro's assessment of the FAC-001-3 Errata was omitted from Assessment Report No. 15, the Panel directs BC Hydro to file a quarterly report listing all the new, revised and retired NERC and Western Electricity Coordinating Council (WECC) reliability standards and Glossary terms approved by FERC, along with the effective dates of the approval. The assessment quarters must be aligned with the Assessment Report Period December 1 to November 30 of the following year. Each quarterly report must be cumulative and must include all new, revised and retired standards listed in prior quarterly reports for the current Assessment Report Period. The quarterly assessment report must be filed with the BCUC by the end of the calendar month following the assessment quarter. The first quarterly filing is due by March 31, 2023, for the Assessment Report Period December 1, 2022 through November 30, 2023.

The report must include, at a minimum, the following information:

1) NERC or WECC Reliability Standard number and title and FERC approval effective date; and
2) BC Hydro's preliminary assessment of:
    i. any adverse impact of the reliability standard on the reliability of electricity transmission in BC if the reliability standard were adopted;
    ii. the suitability of the reliability standard for BC; and
    iii. whether a particular reliability standard is sufficiently critical to reliability that it warrants immediate implementation.

[3] Exhibit B-3, BCUC IR No. 1 to BC Hydro, IR 1.1.1.
[4] Ibid.

4.0 Implementation Plan for EOP-011-2, IRO-010-4 and TOP-003-5

In the Report, BC Hydro recommends a BC-specific implementation plan for reliability standards EOP-011-2, IRO-010-4 and TOP-003-5 (Cold Weather Standards) that would require Entities in BC to be compliant on the first day of the first calendar quarter that is 24 months after adoption by the BCUC.[5]

BC Hydro recommends the effective date for implementation of the Cold Weather Standards for BC Hydro's assets as being the first day of the first calendar quarter that is 18 months after adoption by the BCUC.[6]

FBC recommends a BC-specific implementation plan for the Cold Weather Standards that would be a minimum of 24 months after the standards are adopted by the BCUC. FBC states that budgets and annual maintenance schedules for FBC and third party owned facilities are established annually, typically in the August / September period of each year. FBC states further that in order to implement the Cold Weather Standards revisions within 18 months would require reallocation of 2023 budgets and generator maintenance schedules.[7]

Following the review of feedback from entities, BC Hydro states that the consolidated BC-specific implementation plan for the Cold Weather Standards proposes to require entities in BC to be compliant on the first day of the first calendar quarter that is 24 months after adoption by the BCUC, in order to accommodate the feedback provided by FBC.[8]

FBC had submitted estimated costs and its recommendation of 24 to 36 months for implementation of the Cold Weather Standards in its feedback on the Report, to BC Hydro, by April 2022.[9]

Panel Determination

The Panel notes that the implementation plan for the Cold Weather Standards approved by FERC requires entities in the United States to be compliant on the first day of the first calendar quarter that is 18 months after the standards were approved by FERC.[10]

Pursuant to section 125.2(6) of the UCA, the Panel determines that these reliability standards are required to maintain or achieve consistency between British Columbia and jurisdictions in the United States that have adopted the reliability standards. Entities, including FBC, have been aware of these standards, including the timeframes for implementation, for some time. Given this and the importance of these standards, the Panel further determines that it is reasonable, in the public interest and in the interest of the reliability of the Bulk Electric System in BC, to implement the revised Cold Weather Standards on the first day of the first calendar quarter that is 18 months after the date of adoption of these standards by the BCUC.

[5] Exhibit B-1, Attachment D-2, pg. 1.
[6] Exhibit B-1, Appendix C-1, pp. 3, 5, 8.
[7] Exhibit E-1-1, BCUC IR No. 1 to FBC, IR 1.1.
[8] Exhibit B-3, p.19.
[9] Exhibit B-1, Appendix C-3, pp. 2-4.
[10] https://elibrary.ferc.gov/eLibrary/filelist?document_id=14929910&accessionnumber=20210219-3017.

British Columbia Utilities Commission
Reliability Standards and Glossary Terms Adopted by this Order

Table 1: British Columbia Utilities Commission Reliability Standards with Effective Dates as Adopted

	Standard	Standard Name	Effective Date	Type	BCUC Approved Standard(s) Being Superseded[1]
1	BAL--002--WECC--3	Contingency Reserve	Immediately after BCUC adoption.	Revised	BAL--002--WECC--2a
2	CIP--005--7	Cyber Security — Electronic Security Perimeter(s)	First day of the first calendar quarter that is eighteen (18) months after BCUC adoption. In connection with the recommendation to adopt the standard, BC Hydro recommends that a B.C. specific version of the CIP--005--7, CIP--010--3, CIP--013--2 Implementation Plan be implemented in B.C pursuant to an order of the BCUC providing for the administration of adopted reliability standards.	Revised	CIP--005--6

[1] BCUC approved reliability standard or reliability standard held in abeyance by the BCUC to be superseded by the replacement or revised reliability standard assessed.

	Standard	Standard Name	Effective Date	Type	BCUC Approved Standard(s) Being Superseded[1]
3	CIP--010--4	Cyber Security -- Configuration Change Management and Vulnerability Assessments	First day of the first calendar quarter that is eighteen (18) months after BCUC adoption. In connection with the recommendation to adopt the standard, BC Hydro recommends that a B.C. specific version of the CIP--005--7, CIP--010--3, CIP--013--2 Implementation Plan be implemented in B.C pursuant to an order of the BCUC providing for the administration of adopted reliability standards.	Revised	CIP--010--3
4	CIP--013--2	Cyber Security -- Supply Chain Risk Management	First day of the first calendar quarter that is eighteen (18) months after BCUC adoption. In connection with the recommendation to adopt the standard, BC Hydro recommends that a B.C. specific version of the CIP--005--7, CIP--010--3, CIP--013--2 Implementation Plan be implemented in B.C pursuant to an order of the BCUC providing for the administration of adopted reliability standards.	Revised	CIP--013--1

	Standard	Standard Name	Effective Date	Type	BCUC Approved Standard(s) Being Superseded[1]
5	EOP--011--2	Emergency Preparedness and Operations	Coincide with the effective date of the IRO--010--4 and TOP--003--5 reliability standards after BCUC adoption; the first day of the first calendar quarter that is eighteen (18) months after BCUC adoption. In connection with the recommendation to adopt the standard, BC Hydro recommends that a B.C. specific version of the EOP--011--2, IRO--010--4, and TOP--003--5 Implementation Plan be implemented in B.C pursuant to an order of the BCUC providing for the administration of adopted reliability standards.	Revised	EOP--011--1
6	FAC--008--5	Facility Ratings	First day of the first calendar quarter that is three (3) months after BCUC adoption.	Revised	FAC--008--3
7	FAC--013--1	Establish and Communicate Transfer Capabilities	Retire immediately after BCUC approval.	Retired	N/A; Retired standard
8	INT--004--3.1	Dynamic Transfers	Retire immediately after BCUC approval.	Retired	N/A; Retired standard
9	INT--006--5	Evaluation of Interchange Transactions	Immediately after BCUC adoption.	Revised	INT--006--4
10	INT--009--3	Implementation of Interchange	Immediately after BCUC adoption.	Revised	INT--009--2.1
11	INT--010--2.1	Interchange Initiation and Modification for Reliability	Retire immediately after BCUC approval.	Retired	N/A; Retired standard

	Standard	Standard Name	Effective Date	Type	BCUC Approved Standard(s) Being Superseded[1]
12	INT--011--1.1	Intra--Balancing Authority Transaction Identification	Retire immediately after BCUC approval.	Retired	N/A; Retired standard
13	IRO--002--7	Reliability Coordination -- Monitoring and Analysis	Immediately after BCUC adoption.	Revised	IRO--002--6
14	IRO--010--4	Reliability Coordinator Data Specification and Collection	Coincide with the effective date of the EOP--011--2 and TOP--003--5 reliability standards after BCUC adoption; the first day of the first calendar quarter that is eighteen (18) months after BCUC adoption. In connection with the recommendation to adopt the standard, BC Hydro recommends that a B.C. specific version of the EOP--011--2, IRO--010--4, and TOP--003--5 Implementation Plan be implemented in B.C pursuant to an order of the BCUC providing for the administration of adopted reliability standards.	Revised	IRO--010--3
15	MOD--020--0	Providing Interruptible Demands and Load Management Data to SOs and RCs	Retire immediately after BCUC approval.	Retired	N/A; Retired standard
16	PRC--004--6	Protection System Mis operation Identification and Correction	First day of the first calendar quarter that is three (3) months after BCUC adoption.	Revised	PRC--004--5(i)

	Standard	Standard Name	Effective Date	Type	BCUC Approved Standard(s) Being Superseded[1]
17	PRC--006--5	Automatic Underfrequency Load Shedding	Pending resolution of Planning Coordinator (PC) issues.	Revised	PRC--007--0 and PRC--009--0. PRC--006--4 (Held in abeyance due to suspended Planning Coordinator Assessment Report)
18	TOP--001--5	Transmission Operations	Immediately after BCUC adoption.	Revised	TOP--001--4
19	TOP--003--5	Operational Reliability Data	Coincide with the effective date of the EOP--011--2 and IRO--010--4 reliability standards after BCUC adoption; the first day of the first calendar quarter that is eighteen (18) months after BCUC adoption. In connection with the recommendation to adopt the standard, BC Hydro recommends that a B.C. specific version of the EOP--011--2, IRO--010--4, and TOP--003--5 Implementation Plan be implemented in B.C pursuant to an order of the BCUC providing for the administration of adopted reliability standards.	Revised	TOP--003--4

British Columbia Utilities Commission
Reliability Standards with Effective Dates adopted in British Columbia

Standard	Name	BCUC Order Adopting	Effective Date
BAL-001-2	Real Power Balancing Control Performance	R-14-16	July 1, 2016
BAL-002-3	Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event	R-21-19	April 1, 2020
BAL-002-WECC-2a[1]	Contingency Reserve	R-39-17	July 26, 2017
BAL-002-WECC-3	Contingency Reserve	R-34-22A1	October 29, 2022
BAL-003-2	Frequency Response and Frequency Bias Setting	R-21-21	October 1, 2021
BAL-004-WECC-3	Automatic Time Error Correction	R-21-19	January 1, 2020
BAL-005-1	Balancing Authority Control	R-33-18	October 1, 2019
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	R-33-18	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-003-8	Cyber Security — Security Management Controls	R-19-20	October 1, 2020 and as per B.C-specific Implementation Plan
CIP-004-6	Cyber Security — Personnel & Training	R-39-17	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-005-5[2]	Cyber Security – Electronic Security Perimeter(s)	R-38-15	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-005-6[3]	Cyber Security – Electronic Security Perimeter(s)	R-19-20	April 1, 2023 and as per B.C.-specific Implementation Plan
CIP-005-7	Cyber Security – Electronic Security Perimeter(s)	R-34-22A1	July 1, 2024
CIP-006-6	Cyber Security — Physical Security of BES Cyber Systems	R-39-17	October 1, 2018 and as per B.C.-specific Implementation Plan

[1] Reliability standard is superseded by the revised/replacement reliability standard listed immediately below it as of the effective date(s) of the revised/replacement reliability standard.

[2] Ibid.

[3] Ibid.

Standard	Name	BCUC Order Adopting	Effective Date
CIP-007-6	Cyber Security — System Security Management	R-39-17	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-008-5[4]	Cyber Security – Incident Reporting and Response Planning	R-38-15	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-008-6	Cyber Security – Incident Reporting and Response Planning	R-19-20	April 1, 2023
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	R-39-17	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-010-2[5]	Cyber Security – Configuration Change Management and Vulnerability Assessments	R-39-17	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-010-3[6]	Cyber Security – Configuration Change Management and Vulnerability Assessments	R-19-20	April 1, 2023 and as per B.C.-specific Implementation Plan
CIP-010-4	Cyber Security – Configuration Change Management and Vulnerability Assessments	R-34-22A1	July 1, 2024
CIP-011-2	Cyber Security – Information Protection	R-39-17	October 1, 2018 and as per B.C.-specific Implementation Plan
CIP-012-1	Cyber Security – Communications between Control Centers	R-21-21	October 1, 2023
CIP-013-1[7]	Cyber Security - Supply Chain Risk Management	R-19-20	April 1, 2023 and as per B.C.-specific Implementation Plan
CIP-013-2	Cyber Security - Supply Chain Risk Management	R-34-22A1	July 1, 2024
CIP-014-2	Physical Security	R-32-16A	October 1, 2017 and as per B.C.-specific Implementation Plan
COM-001-3	Communications	R-39-17	R1, R2: October 1, 2017 R3-R13: October 1, 2018

[4] Reliability standard is superseded by the revised/replacement reliability standard listed immediately below it as of the effective date(s) of the revised/replacement reliability standard.

[5] Ibid.

[6] Ibid.

[7] Ibid.

Standard	Name	BCUC Order Adopting	Effective Date
COM-002-4	Operating Personnel Communications Protocols	R-32-16A	April 1, 2017
EOP-003-1[8]	Load Shedding Plans	G-67-09	November 1, 2010
EOP-003-2[9]	Load Shedding Plans	N/A	Adoption held in abeyance at this time[10]
EOP-004-4	Event Reporting	R-21-19	October 1, 2020
EOP-005-3	System Restoration and Blackstart Resources	R-21-19	October 1, 2020
EOP-006-3	System Restoration Coordination	R-21-19	October 1, 2020
EOP-008-2	Loss of Control Center Functionality	R-21-19	October 1, 2020
EOP-010-1	Geomagnetic Disturbance Operations	R-38-15	R1, R3: October 1, 2016 R2: October 1, 2017
EOP-011-1[11]	Emergency Operations	R-39-17	October 1, 2018
EOP-011-2	Emergency Preparedness and Operations	R-34-22A1	July 1, 2024
FAC-001-3	Facility Interconnection Requirements	R-33-18	October 1, 2019
FAC-002-3	Facility Interconnection Studies	R-21-21	January 1, 2022
FAC-003-4	Transmission Vegetation Management	R-39-17	October 1, 2017
FAC-008-3[12]	Facility Ratings	R-32-14	August 1, 2015 R4 and R5: Retired January 21, 2014[13]
FAC-008-5	Facility Ratings	R-34-22A1	April 1, 2023
FAC-010-3	System Operating Limits Methodology for the Planning Horizon	R-39-17	R1–R4: October 1, 2017 R5: Retired

[8] Reliability standard would be superseded by EOP-003-2 if adopted in B.C. Adoption of EOP-003-2 pending reassessment.

[9] Reliability standard is superseded by EOP-011-1 as of the EOP-011-1 effective date in conjunction with PRC-010-2 Requirement 1 if adopted in B.C. Adoption of PRC-010-2 is held in abeyance at this time.

[10] On January 26, 2022, the BCUC Reasons for Decision for Order No. R-4-22, indicated that a separate proceeding would be initiated regarding Planning Coordinator issues and adjourned the Planning Coordinator Assessment Report.

[11] Reliability standard is superseded by the revised/replacement reliability standard listed immediately below it as of the effective date(s) of the revised/replacement reliability standard.

[12] Reliability standard is superseded by the revised/replacement reliability standard listed immediately below it as of the effective date(s) of the revised/replacement reliability standard.

[13] On November 21, 2013, FERC Order 788 (referred to as Paragraph 81) approved the retiring of the reliability standard requirements.

Standard	Name	BCUC Order Adopting	Effective Date
FAC-011-3	System Operating Limits Methodology for the Operations Horizon	R-39-17	October 1, 2017
FAC-013-1[14]	Establish and Communicate Transfer Capability	G-67-09	November 1, 2010 Retired: October 29, 2022
FAC-013-2	Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon	N/A	Adoption held in abeyance at this time[15]
FAC-014-2	Establish and Communicate System Operating Limits	G-167-10	January 1, 2011
FAC-501-WECC-2	Transmission Maintenance	R-21-19	October 1, 2019
INT-004-3.1	Dynamic Transfers	R-38-15	R1, R2: October 1, 2015 R3: January 1, 2016 Retired: October 29, 2022
INT-006-4[16]	Evaluation of Interchange Transactions	R-38-15	October 1, 2015
INT-006-5	Evaluation of Interchange Transactions	R-34-22A1	October 29, 2022
INT-009-2.1[1]	Implementation of Interchange	R-38-15	October 1, 2015
INT-009-3	Implementation of Interchange	R-34-22A1	October 29, 2022
INT-010-2.1	Interchange Initiation and Modification for Reliability	R-38-15	October 1, 2015 Retired: October 29, 2022
INT-011-1.1	Intra-Balancing Authority Transaction Identification	R-38-15	October 1, 2015 Retired: October 29, 2022
IRO-001-4	Reliability Coordination – Responsibilities	R-39-17	October 1, 2017
IRO-002-6[1]	Reliability Coordination – Monitoring and Analysis	R-19-20	April 1, 2021
IRO-002-7	Reliability Coordination – Monitoring and Analysis	R-34-22A1	October 29, 2022

[14] Reliability standard is superseded by the revised/replacement reliability standard listed immediately below it as of the effective date(s) of the revised/replacement reliability standard.

[15] On October 15, 2020, FERC Order No. 873 approved the retirement of the reliability standard in the United States. The reliability standard was not recommended for adoption in B.C. per the Planning Coordinator Assessment Report filed with BCUC on May 31, 2021.

[16] Reliability standard is superseded by the revised/replacement reliability standard listed immediately below it as of the effective date(s) of the revised/replacement reliability standard.

Standard	Name	BCUC Order Adopting	Effective Date
IRO-005-3.1a[17]	Reliability Coordination - Current Day Operations	R-32-14	August 1, 2014
IRO-006-5	Reliability Coordination – Transmission Loading Relief	R-1-13	April 15, 2013
IRO-006-WECC-3	Qualified Transfer Path Unscheduled Flow (**USF**) Relief	R-19-20	January 1, 2021
IRO-008-2	Reliability Coordinator Operational Analyses and Real-time Assessments	R-39-17	October 1, 2017
IRO-009-2	Reliability Coordinator Actions to Operate Within IROLs	R-39-17	October 1, 2017
IRO-010-3[1]	Reliability Coordinator Data Specification and Collection	R-21-21	January 1, 2022
IRO-010-4	Reliability Coordinator Data Specification and Collection	R-34-22A1	July 1, 2024
IRO-014-3	Coordination Among Reliability Coordinators	R-39-17	October 1, 2017
IRO-017-1	Outage Coordination	R-39-17	October 1, 2020
IRO-018-1(i)	Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities	R-33-18	April 1, 2020
MOD-001-1a	Available Transmission System Capability	G-175-11	November 30, 2011
MOD-004-1	Capacity Benefit Margin	G-175-11	November 30, 2011
MOD-008-1	Transmission Reliability Margin Calculation Methodology	G-175-11	November 30, 2011
MOD-010-0[18]	Steady-State Data for Modeling and Simulation for the Interconnected Transmission System	G-67-09	November 1, 2010
MOD-012-0[18]	Dynamics Data for Modeling and Simulation of the Interconnected Transmission System	G-67-09	November 1, 2010
MOD-020-0	Providing Interruptible Demands and Direct Control Load Management Data to System Operators and Reliability Coordinators	G-67-09	November 1, 2010 Retired: October 29, 2022

[17] Refer to "IRO and TOP Reliability Standards Supersession Mapping" section below.

[18] Reliability standard will be superseded by Requirement 2 of MOD-032-1 by the effective date of MOD-032-1 Requirement 2, pending adoption in B.C.

Standard	Name	BCUC Order Adopting	Effective Date
MOD-025-2	Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability	R-38-15 With revised effective dates by Order R-14-20	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by April 1, 2021
MOD-026-1	Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions	R-38-15	R1: October 1, 2016 R2: 30% by October 1, 2019 50% by October 1, 2021 100% by October 1, 2025 R3-R6: October 1, 2015
MOD-027-1	Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions	R-38-15	R1: October 1, 2016 R2: 30% by October 1, 2019 50% by October 1, 2021 100% by October 1, 2025 R3-R5: October 1, 2015
MOD-028-2	Area Interchange Methodology	R-32-14	August 1, 2014
MOD-029-2a	Rated System Path Methodology	R-39-17	October 1, 2017
MOD-030-3	Flowgate Methodology	R-39-17	October 1, 2017
MOD-031-3	Demand and Energy Data	R-21-21	January 1, 2022
MOD-032-1	Data for Power System Modeling and Analysis	R-38-15	Adoption held in abeyance at this time[10]
MOD-033-1	Steady-State and Dynamic System Model Validation	R-38-15	Adoption held in abeyance at this time[10]
NUC-001-4	Nuclear Plant Interface Coordination	R-21-21	October 1, 2021
PER-003-2	Operating Personnel Credentials	R-21-19	April 1, 2020
PER-005-2	Operations Personnel Training	R-38-15	R1-R4, R6: October 1, 2016 R5: October 1, 2017
PER-006-1	Specific Training for Personnel	R-21-19	October 1, 2021
PRC-002-2	Disturbance Monitoring and Reporting Requirements	R-32-16A	R1, R5: April 1, 2017 R2-R4, R6-R11: staged as per B.C.-specific Implementation Plan R12: July 1, 2017
PRC-004-5(i)[1]	Protection System Misoperation Identification and Correction	R-32-16A	October 1, 2017
PRC-004-6	Protection System Misoperation Identification and Correction	R-34-22A1	April 1, 2023

Standard	Name	BCUC Order Adopting	Effective Date
PRC-005-1.1b[1, 19]	Transmission and Generation Protection System Maintenance and Testing	R-32-14	January 1, 2015
PRC-005-6	Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance	R-39-17	R1, R2, R5: October 1, 2019 R3, R4: See B.C.-specific Implementation Plan
PRC-006-4[1]	Automatic Underfrequency Load Shedding	N/A	Adoption held in abeyance at this time[10]
PRC-006-5	Automatic Underfrequency Load Shedding	N/A	To be determined[20]
PRC-007-0[21]	Assuring consistency of entity Underfrequency Load Shedding Program Requirements	G-67-09	November 1, 2010
PRC-008-0[19]	Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program	G-67-09	November 1, 2010
PRC-009-0[21]	Analysis and Documentation of Underfrequency Load Shedding Performance Following an Underfrequency Event	G-67-09	November 1, 2010
PRC-010-0[1]	Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program	G-67-09	November 1, 2010 R2: Retired January 21, 2014[13]
PRC-010-2	Under Voltage Load Shedding	N/A	Adoption held in abeyance at this time[10]
PRC-011-0[19]	Undervoltage Load Shedding system Maintenance and Testing	G-67-09	November 1, 2010
PRC-012-2	Remedial Action Schemes	R-33-18	October 1, 2021 R1: Attachment 1, Section II Parts 6(d) and 6(e) to be determined.[10] R2: Attachment 2, Section I Parts 7(d) and 7(e) to be determined.[10] R4: To be determined.[10]

[19] Reliability standard is superseded by PRC-005-6 as per the PRC-005-6 B.C. specific Implementation Plan.

[20] On January 26, 2022, the BCUC Reasons for Decision for Order No. R-4-22, indicated that a separate proceeding would be initiated regarding Planning Coordinator issues and adjourned the Planning Coordinator Assessment Report.

[21] Reliability standard will be superseded by PRC-006-4 if adopted in B.C.

Standard	Name	BCUC Order Adopting	Effective Date
PRC-017-1[19]	Remedial Action Scheme Maintenance and Testing	R-39-17	October 1, 2017
PRC-018-1[22]	Disturbance Monitoring Equipment Installation and Data Reporting	G-67-09	November 1, 2010
PRC-019-2	Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection	R-32-16A With revised effective dates by Order R-14-20	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by April 1, 2021
PRC-021-1[23]	Under Voltage Load Shedding Program Data	G-67-09	November 1, 2010
PRC-022-1[23]	Under Voltage Load Shedding Program Performance	G-67-09	November 1, 2010 R2: Retired January 21, 2014[13]
PRC-023-2[1, 24]	Transmission Relay Loadability	R-41-13	R1-R5: For circuits identified by sections 4.2.1.1 and 4.2.1.4: January 1, 2016 For circuits identified by sections 4.2.1.2, 4.2.1.3, 4.2.1.5, and 4.2.1.6: To be determined[10] R6: To be determined[10]
PRC-023-4	Transmission Relay Loadability	R-39-17	R1-R5 Circuits 4.2.1.1, 4.2.1.4: October 1, 2017 with the exception of Criterion 6 of R1 which will not become effective until PRC-025-2 R1 is completely effective in B.C. Until then, PRC-023-2 R1, Criterion 6 will remain in effect. R1-R5 Circuits 4.2.1.2, 4.2.1.3, 4.2.1.5, 4.2.1.6 and R6: To be determined.[10]
PRC-024-2[1]	Generator Frequency and Voltage Protective Relay Settings	R-32-16A With revised effective dates by Order R-14-20	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by April 1, 2021

[22] Reliability standard is superseded by PRC-002-2 as of the PRC-002-2 effective date.

[23] Reliability standard is superseded by PRC-010-2 if adopted in B.C.

[24] PRC-023-2 Requirement 1, Criterion 6 only is superseded by PRC-025-2 as of PRC-025-2's 100 per cent Effective Date.

Standard	Name	BCUC Order Adopting	Effective Date
PRC-024-3	Frequency and Voltage Protection Settings for Generating Resources	R-21-21	October 1, 2023
PRC-025-2	Generator Relay Loadability	R-21-19	October 1, 2019 and staged per B.C. specific Implementation Plan
PRC-026-1	Relay Performance During Stable Power Swings	N/A	Adoption held in abeyance at this time[10]
PRC-027-1	Coordination of Protection Systems for Performance During Faults	R-21-19	October 1, 2021
TOP-001-1a[17]	Reliability Responsibilities and Authorities	R-1-13	January 15, 2013
TOP-001-4[1]	Transmission Operations	R-33-18 With revised effective dates by Order R-14-20	April 1, 2021
TOP-001-5	Transmission Operations	R-34-22A1	October 29, 2022
TOP-002-4	Operations Planning	R-39-17 With revised effective dates by Order R-14-20	April 1, 2021
TOP-003-4[1]	Operational Reliability Data	R-21-21	January 1, 2022
TOP-003-5	Operational Reliability Data	R-34-22A1	July 1, 2024
TOP-007-0[17]	Reporting System Operating Unit (**SOL**) and Interconnection Reliability Operating Limit (**IROL**) Violations	G-67-09	November 1, 2010
TOP-008-1[17]	Response to Transmission Limit Violations	G-67-09	November 1, 2010
TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities	R-33-18 With revised effective dates by Order R-14-20	April 1, 2021
TPL-001-4[1]	Transmission System Planning Performance Requirements	R-27-18A	R1: July 1, 2019 R2-R6, R8: July 1, 2020 R7: To be determined[10]
TPL-001-5.1	Transmission System Planning Performance Requirements	N/A	Adoption held in abeyance at this time.[10]
TPL-007-4	Transmission System Planned Performance for Geomagnetic Disturbance Events	N/A	Adoption held in abeyance at this time[10]

Standard	Name	BCUC Order Adopting	Effective Date
VAR-001-5	Voltage and Reactive Control	R-21-19	October 1, 2019
VAR-002-4.1	Generator Operation for Maintaining Network Voltage Schedules	R-33-18	October 1, 2018
VAR-501-WECC-3.1	Power System Stabilizer (**PSS**)	R-33-18	October 1, 2020 R3: For units placed into service after the effective date: January 1, 2021 For units placed into service prior to the effective date: January 1, 2024

British Columbia Utilities Commission

IRO and TOP Reliability Standards
Supersession Mapping

This following mapping shows the supersession of Requirements for the following IRO and TOP reliability standards by the revised/replacement reliability standards indicated which are either adopted or yet to be adopted in B.C. as of the effective date in the "B.C. Reliability Standards" section above:

IRO-005-3.1a	—	Reliability Coordination - Current Day Operations
TOP-001-1a	—	Reliability Responsibilities and Authorities
TOP-007-0	—	Reporting System Operating Limit (**SOL**) and Interconnection Reliability Operating Limit (**IROL**) Violations
TOP-008-1	—	Response to Transmission Limit Violations

Standard IRO-005-3.1a — Reliability Coordination - Current Day Operations	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirements R1-R3	IRO-002-6
Requirement R4	IRO-008-2
Requirements R5 and R8	IRO-001-4 IRO-002-6
Requirements R6 and R7	IRO-008-2 IRO-017-1
Requirement R8	IRO-001-4 IRO-002-6
Requirement R9	IRO-002-6 IRO-010-2
Requirement R10	IRO-009-1 TOP-001-4
Requirement R11	MOD-001-2, Requirement R2 (pending FERC adoption in the U.S. and subsequent assessment and adoption in B.C.)
Requirement R12	IRO-008-2

Standard TOP-001-1a — Reliability Responsibilities and Authorities	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirements R1, R2, R4, R5, R6	TOP-001-4
Requirement R3	IRO-001-4 TOP-001-4
Requirement R7	TOP-001-4 TOP-003-3 IRO-010-2
Requirement R8	EOP-003-2, Requirement 1 (adoption held in abeyance in B.C. due to PA/PC dependencies) IRO-009-2

Standard TOP-007-0 — Reporting System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirement R1	IRO-008-2 TOP-001-4
Requirement R2	IRO-009-2 TOP-001-4
Requirement R3	EOP-003-2, Requirement 1 (adoption held in abeyance in B.C. due to PA/PC dependencies) IRO-009-2
Requirement R4	IRO-008-2

Standard TOP-008-1 — Response to Transmission Limit Violations	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirements R1	EOP-003-2, Requirement 1 (adoption held in abeyance in B.C. due to PA/PC dependencies) TOP-001-4
Requirements R2 and R3	TOP-001-4
Requirement R4	TOP-001-4 TOP-002-4 TOP-003-3

British Columbia (B.C.) Exceptions to the Glossary of Terms Used in North American Electric Reliability Corporation (NERC) Reliability Standards (NERC Glossary)

Updated by Order R-34-22A1, dated October 28, 2022

Introduction:

This document is to be used in conjunction with the NERC Glossary dated June 28, 2021.

- The NERC Glossary terms listed in Table 1 below are effective in B.C. on the date specified in the "Effective Date" column.
- Table 2 below outlines the adoption history by the BCUC of the NERC Glossaries in B.C.
- Any NERC Glossary terms and definitions in the NERC Glossary that are not approved by FERC on or before November 30, 2021 are of no force or effect in B.C.
- Any NERC Glossary terms that have been remanded or retired by NERC are of no force or effect in B.C., with the exception of those remanded or retired NERC Glossary terms which have not yet been retired in B.C.
- The Electric Reliability Council of Texas, Northeast Power Coordinating Council and Reliability First regional definitions listed at the end of the NERC Glossary have been adopted by the NERC Board of Trustees for use in regional standards and are of no force or effect in B.C.

Table 1: B.C. Effective Date Exceptions to Definitions in the October 8, 2020 Version of the NERC Glossary

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Actual Frequency (F_A)	-	Report No. 11	R-33-18	Adoption	October 1. 2019
Actual Net Interchange (NI_A)	-	Report No. 11	R-33-18	Adoption	October 1, 2019
Automatic Time Error Correction (I_{ATEC})	-	Report No. 11	R-33-18	Adoption	October 1, 2019
Adjacent Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Alternative Interpersonal Communication	-	Report No. 9	R-32-16A	Adoption	October 1, 2017
Area Control Error (from NERC section of the Glossary)	ACE	Report No. 7	R-32-14	Adoption	October 1, 2014
Area Control Error (from the WECC Regional Definitions section of the Glossary)	ACE	Report No. 7	R-32-14	Retirement	October 1, 2014
Arranged Interchange	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Attaining Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Automatic Generation Control	AGC	Report No. 11	R-33-18	Adoption	October 1, 2019
Automatic Time Error Correction	-	Report No. 7	R-32-14	Adoption	October 1, 2014
Balancing Authority	-	Report No. 11	R-33-18	Adoption	January 1, 2019
Balancing Contingency Event[1]	-	Report No. 10	R-39-17	Adoption	January 1, 2018

[1] FERC approved terms in the NERC Glossary of Terms as of February 7, 2017; intended for BAL-002-2.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
BES Cyber Asset[2]	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
BES Cyber Asset	BCA	Report No. 10	R-39-17	Adoption	October 1, 2018
BES Cyber System	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
BES Cyber System Information	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Blackstart Capability Plan	-	Report No. 7	R-32-14	Retirement	August 1, 2015
Blackstart Resource[2]	-	Report No. 6	R-41-13	Adoption	December 12, 2013
Blackstart Resource	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Bulk Electric System	BES	Report No. 8	R-38-15	-	October 1, 2015
Bulk-Power System[2]	-	Report No. 8	R-38-15	-	October 1, 2015
Bulk-Power System	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Bus-tie Breaker	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Cascading	-	Report No. 10	R-39-17	Adoption	October 1, 2017

[2] NERC Glossary term definition is superseded by the revised NERC Glossary term definition listed immediately below it as of the effective date(s) of the revised NERC Glossary term definition.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
CIP Exceptional Circumstance	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
CIP Senior Manager	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Composite Confirmed Interchange	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Confirmed Interchange	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Composite Protection System	-	Report No. 9	R-32-16A	Adoption	October 1, 2017
Consequential Load Loss	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Contingency Event Recovery Period[1]	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Contingency Reserve[1]	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Contingency Reserve Restoration Period[1]	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Contributing Schedule (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020
Control Center	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Critical Assets	-	Report No. 9	R-32-16A	Retirement	September 30, 2018
Critical Cyber Assets	-	Report No. 9	R-32-16A	Retirement	September 30, 2018
Cyber Assets	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Cyber Security Incident	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Cyber Security Incident	-	Report No. 13	R-19-20	Adoption	April 1, 2023
Demand-Side Management	DSM	Report No. 9	R-32-16A	Adoption	October 1, 2016
Dial-up Connectivity	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Distribution Provider	DP	Report No. 10	R-39-17	Adoption	October 1, 2017
Disturbance	-	Report No. 11	R-33-18	Retirement	October 1, 2018
Dynamic Interchange Schedule or Dynamic Schedule	-	Report No. 8	R-38-15	Adoption	October 1, 2015

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Electronic Access Control or Monitoring Systems	EACMS	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Electronic Access Point	EAP	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Electronic Security Perimeter	ESP	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Element	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Energy Emergency[2]	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Energy Emergency	-	Report No. 11	R-33-18	Retirement	October 1, 2018
External Routable Connectivity	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Frequency Bias Setting	-	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Frequency Response Measure	FRM	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced
Frequency Response Obligation	FRO	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced
Frequency Response Sharing Group	FRSG	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced
Generator Operator	GOP	Report No. 10	R-39-17	Adoption	October 1, 2017
Generator Owner	GO	Report No. 10	R-39-17	Adoption	October 1, 2017
Geomagnetic Disturbance Vulnerability Assessment or GMD Vulnerability Assessment	GMD	Report No. 10	R-39-17	Adoption	To be determined[3]
Interactive Remote Access	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Interchange Authority	IA	Report No. 10	R-39-17	Adoption	October 1, 2017
Interchange Meter Error (IME)	-	Report No. 11	R-33-18	Adoption	October 1, 2019
Interconnected Operations Service	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Interconnection	-	Report No. 10	R-39-17	Adoption	October 1, 2017

[3] The NERC Glossary term is associated with reliability standard that is dependent on the Planning Authority/Planning Coordinator function. The BCUC Reasons for Decision for Order No. R-41-13 (page 20), indicated that a separate process would be established to consider this matter as it pertains to B.C.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Interconnection Reliability Operating Limit	IROL	Report No. 6	R-41-13	Adoption	December 12, 2013
Intermediate Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Intermediate System	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Interpersonal Communication	-	Report No. 9	R-32-16A	Adoption	October 1, 2017
Load-Serving Entity	LSE	Report No. 10	R-39-17	Adoption	October 1, 2017
Long-Term Transmission Planning Horizon	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Minimum Vegetation Clearance Distance	MVCD	Report No. 7	R-32-14	Adoption	August 1, 2015
Misoperation	-	Report No. 9	R-32-16A	Adoption	October 1, 2017
Most Severe Single Contingency[1]	MSSC	Report No. 10	R-39-17	Adoption	January 1, 2018
Native Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Non-Consequential Load Loss	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Non-Spinning Reserve	-	Report No. 11	R-33-18	Retirement	October 1, 2018
Operating Instruction	-	Report No. 9	R-32-16A	Adoption	April 1, 2017
Operational Planning Analysis[2]	-	Report No. 6	R-41-13	Adoption	December 12, 2013
Operational Planning Analysis[2]	-	Report No. 8	R-38-15	Adoption	October 1, 2015

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Operational Planning Analysis[2]	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Operational Planning Analysis	OPA	Report No. 12	R-21-19	Adoption	October 1, 2021
Operations Support Personnel	-	Report No. 8	R-38-15	Adoption	Align with effective date of Requirement 5 of the PER-005-2 standard where this term is referenced
Physical Access Control Systems	PACS	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Physical Security Perimeter	PSP	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Planning Assessment	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Planning Authority	PA	Report No. 10	R-39-17	Adoption	October 1, 2017
Point of Receipt	POR	Report No. 10	R-39-17	Adoption	October 1, 2017
Pre-Reporting Contingency Event ACE Value[1]	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Protected Cyber Assets[2]	PCA	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Protected Cyber Assets	PCA	Report No. 10	R-39-17	Adoption	October 1, 2018

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Protection System	-	Report No. 6	R-41-13	Adoption	January 1, 2015 for each entity to modify its protection system maintenance and testing program to reflect the new definition (to coincide with recommended effective date of PRC-005-1b) and until the end of the first complete maintenance and testing cycle to implement any additional maintenance and testing for battery chargers as required by that entity's program.
Protection System Coordination Study	-	Report No. 12	R-21-19	Adoption	October 1, 2021
Protection System Maintenance Program	PSMP	Report No. 8	R-38-15	Adoption	Align with effective date of Requirement 1 of the PRC-005-2 standard where this term is referenced
Protection System Maintenance Program *(PRC-005-6)*	PSMP	Report No. 10	R-39-17	Adoption	October 1, 2019
Pseudo-Tie[2]	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Pseudo-Tie	-	Report No. 11	R-33-18	Adoption	January 1, 2019
Qualified Controllable Device (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020
Qualified Path (WECC Regional Term)	-	Report No. 13	R-19-20	Adoption	January 1, 2021
Qualified Transfer Path (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020
Qualified Transfer Path Curtailment Event (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Reactive Power	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Real Power	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Real-time Assessment[2]	-	Report No. 6	R-41-13	Adoption	January 1, 2014
Real-time Assessment[2]	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Real-time Assessment	RTA	Report No. 12	R-21-19	Adoption	October 1, 2021
Reliability Adjustment Arranged Interchange	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Reliability Coordinator	RC	Report No. 10	R-39-17	Adoption	October 1, 2017
Reliability Directive	-	Report No. 9	R-32-16A	Retirement	July 18, 2016
Reliability Standard[2]	-	Report No. 8	R-32-14	Adoption	October 1, 2015
Reliability Standard	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Reliable Operation[2]	-	Report No. 8	R-32-14	Adoption	October 1, 2015
Reliable Operation	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Relief Requirement (WECC Regional Term)	-	Report No. 8	R-38-15	Adoption	Align with effective date of IRO-006-WECC-2 standard where this term is referenced
Relief Requirement (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020
Remedial Action Scheme[2]	RAS	Report No. 1	G-67-09	Adoption	June 4, 2009
Remedial Action Scheme	RAS	Report No. 9		-	To be determined[3]
Removable Media[2]	-	Report No. 10	R-39-17	Adoption	October 1, 2018
Removable Media	-	Report No. 12	R-21-19	Adoption	October 1, 2019
Reporting ACE	-	Report No. 11	R-33-18	Adoption	October 1, 2019

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Reportable Balancing Contingency Event[1]	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Reportable Cyber Security Incident	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Reportable Cyber Security Incident	-	Report No. 13	R-19-20	Adoption	April 1, 2023
Request for Interchange	RFI	Report No. 8	R-38-15	Adoption	October 1, 2015
Reserve Sharing Group	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Reserve Sharing Group Reporting ACE[1]	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Resource Planner	RP	Report No. 10	R-39-17	Adoption	October 1, 2017
Scheduled Net Interchange (NI_S)	-	Report No. 11	R-33-18	Adoption	October 1, 2019
Sink Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Source Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Special Protection System (Remedial Action Scheme) [2]	SPS	Report No. 1	G-67-09	Adoption	June 4, 2009
Special Protection System (Remedial Action Scheme)	SPS	Report No. 10	R-39-17	Adoption	Held in abeyance due to PC dependencies
Spinning Reserve	-	Report No. 11	R-33-18	Retirement	October 1, 2018
System Operating Limit	-	Report No. 10	R-39-17	Adoption	October 1, 2017

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
System Operator	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) as reference is made to the term Control Center as part of the definition of System Operator. The term Control Center is in turn referenced from the CIP Version 5 standards.
Total Internal Demand	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Transient Cyber Asset[2]	-	Report No. 10	R-39-17	Adoption	October 1, 2018
Transient Cyber Asset	TCA	Report No. 12	R-21-19	Adoption	October 1, 2019
Transmission Customer	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Transfer Distribution Factor (WECC Regional Term)	TDF	Report No. 13	R-19-20	Retirement	December 31, 2020
Transmission Operator	TOP	Report No. 10	R-39-17	Adoption	October 1, 2017
Transmission Owner	TO	Report No. 10	R-39-17	Adoption	October 1, 2017
Transmission Planner	TP	Report No. 10	R-39-17	Adoption	October 1, 2017
Transmission Service Provider	TSP	Report No. 10	R-39-17	Adoption	October 1, 2017
Under Voltage Load Shedding Program	-	Report No. 9		-	To be determined[3]
Right-of-Way	ROW	Report No. 7	R-32-14	Adoption	August 1, 2015
TLR (Transmission Loading Relief) Log	-	Report No. 7	R-32-14	Adoption	August 1, 2014
Vegetation Inspection	-	Report No. 7	R-32-14	Adoption	August 1, 2015

Table 2 NERC Glossary Adoption History in B.C.

NERC Glossary of Terms Version Date	Assessment Report Number	BCUC Order Adoption Date	BCUC Order Adopting	Notes Pertaining to NERC Glossary Effective Date
February 12, 2008	Report No. 1	June 4, 2009	G-67-09	1. The NERC Glossaries listed became effective as of the date of the respective BCUC Orders adopting them. See the exception of the BAL-001-2 Glossary Terms within the NERC Glossary dated December 7, 2015.[1] 2. Specific effective dates of new and revised NERC Glossary terms adopted in a BCUC Order appear in attachments to the Order. Each Glossary term to be superseded by a revised Glossary term adopted in the Order shall remain in effect until the effective date of the Glossary term superseding it. 3. NERC Glossary terms which have not been approved by FERC are of no force or effect in B.C. 4. Any NERC Glossary terms that have been remanded or retired by NERC are of no force or effect in B.C., with the exception of those remanded or retired NERC Glossary terms which have not yet been retired in B.C. 5. The Electric Reliability Council of Texas, Northeast Power Coordinating Council and Reliability First regional definitions listed at the end of the NERC Glossary of Terms are of no force or effect in B.C.
April 20, 2010	Report No. 2	November 10, 2010	G-167-10	
August 4, 2011	Report No. 3	September 1, 2011	G-162-11 replacing G-151-11	
December 13, 2011	Report No. 5	January 15, 2013	R-1-13	
December 5, 2012	Report No. 6	December 12, 2013	R-41-13	
January 2, 2014	Report No. 7	July 17, 2014	R-32-14	
October 1, 2014	Report No. 8	July 24, 2015	R-38-15	
December 7, 2015	BAL-001-2	April 21, 2016	R-14-16	
December 7, 2015	Report No. 9[2]	July 18, 2016	R-32-16A	
November 28, 2016	Report No. 10	July 26, 2017	R-39-17	
November 28, 2016	TPL-001-4	June 28, 2018	R-27-18A	
October 6, 2017	Report No. 11	October 1, 2018	R-33-18	
July 3, 2018	Report No.12	September 26, 2019	R-21-19	
August 12, 2019	Report No. 13	September 8, 2020	R-19-20	
October 8, 2020	Report No. 14	September 21, 2021	R-21-21	
June 28, 2021	Report No. 15			

British Columbia Utilities Commission

Implementation Plan for Cyber Security Supply Chain Risk Management Associated Standards

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 Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2

Each Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the BCUC order approving the Reliability Standard.

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 the CIP Version 5 standards per BCUC Order R-38-15. The Implementation Plan associated with the CIP Version 5 standards provides as follows:

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-002-5.1a, 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-002-5.1a, 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- 002-5.1a, 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-002-5.1a, 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-002-5.1a 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 British Columbia.

British Columbia Utilities Commission

Implementation Plan for Cold Weather Associated Standards

Applicable Standard(s)

- EOP-011-2 – Emergency Preparedness and Operations
- IRO-010-4 – Reliability Coordinator Data Specification and Collection
- TOP-003-5 – Operational Reliability Data

Requested Retirement(s)

- EOP-011-1 – Emergency Operations
- IRO-010-3 – Reliability Coordinator Data Specification and Collection
- TOP-003-4 – Operational Reliability Data

Applicable Entities

- See subject Reliability Standards.

Background

In July 2019, FERC and NERC staff released a joint report titled *The South Central United States Cold Weather Bulk Electronic System Event of January 17, 2018.* [1] Following the publication of the report, a Standard Authorization Request[2] was submitted to review and address the recommendations in the report, including:

1. Generator Owner or Generator Operator develops and implements cold weather preparedness plans, procedures, and awareness training based on factors such as geographical location and plant configurations, which 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; and
    c. Performing periodic maintenance and inspection of freeze protection measures.
2. Balancing Authority, Reliability Coordinators, or Transmission Operators, as applicable will include in its data specifications that the Generator Owner or Generator Operator will provide its BES generating unit's associated design specification or historical demonstrated performance and operating limitations during cold weather.

[1] Link to report: https://www.nerc.com/pa/rrm/ea/Documents/South_Central_Cold_Weather_Event_FERC-NERC-Report_20190718.pdf
[2] Link to SAR: https://www.nerc.com/pa/Stand/Project%20201906%20Cold%20Weather%20DL/2019-06_Cold_Weather_SAR_Clean_02192020.pdf

3. Balancing Authority, Reliability Coordinators, or Transmission Operators, as applicable will include in their data specifications that the Generator Owner or Generator Operator will provide a notification when local forecasted cold weather conditions are expected to limit BES generating unit capability or 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 their Operating Plans, or determine the expected availability of contingency reserves for the appropriate next day operating horizon.

The Reliability Standard revisions proposed by this project will help enhance the reliability of the Bulk Power System during cold weather events, and mitigate the potential for generating unit unavailability due to lack of preparation for cold weather periods by providing increased visibility of cold weather related data to the Reliability Coordinators, Balancing Authorities, and Transmission Operators, and by requiring a baseline level of cold weather planning and preparation by Generator Owners.

General Considerations

This implementation plan provides that entities shall have eighteen months to become compliant with the revised Reliability Standards. This implementation plan reflects consideration that entities will need time to develop, implement, and maintain cold weather preparedness plan(s) for its generating site(s). In addition, entities may need time identifying cold weather operating temperatures through engineering studies as permitted under Reliability Standard EOP-011-2. This implementation plan also reflects consideration that entities will need time to develop, and distribute revised data specifications to affected entities, and for receiving entities to develop the necessary capabilities in order to comply with revised data specifications.

Effective Dates

Reliability Standard EOP-011-2

The Reliability Standard shall become effective on the first day of the first calendar quarter that is eighteen (18) months after the effective date of the BCUC order approving the Reliability Standard.

Reliability Standard IRO-010-4

The Reliability Standard shall become effective on the first day of the first calendar quarter that is eighteen (18) months after the effective date of the BCUC order approving the Reliability Standard.

Reliability Standard TOP-003-5

The Reliability Standard shall become effective on the first day of the first calendar quarter that is eighteen (18) months after the effective date of the BCUC order approving the Reliability Standard.

Retirement Dates

Reliability Standard EOP-011-1

Reliability Standard EOP-011-1 shall be retired immediately prior to the effective date of Reliability Standard EOP-011-2 in British Columbia.

Reliability Standard IRO-010-3

Reliability Standard IRO-010-3 shall be retired immediately prior to the effective date of Reliability Standard IRO-010-4 in British Columbia.

Reliability Standard TOP-003-4
Reliability Standard TOP-003-4 shall be retired immediately prior to the effective date of Reliability Standard TOP-003-5 in British Columbia.

Initial Performance of Periodic Requirements
Responsible Entities shall develop, maintain, and implement the Operating Plan(s) required by Reliability Standard EOP-011-2 by the effective date of the Reliability Standard. For the cold weather preparedness plan(s) for generating unit(s) required under EOP-011-2 Requirement R7, the Responsible Entity shall perform annual inspection and maintenance of generating unit freeze protection measures under EOP-011-2 Requirement R7 Part 7.2 and conduct generating unit specific training for its maintenance and operations personnel under EOP-011-2 Requirement R8 by the effective date of the Reliability Standard.

A. Introduction

1. Title: **Contingency Reserve**

2. Number: BAL-002-WECC-3

3. Purpose: To specify the quantity and types of Contingency Reserve required to ensure reliability under normal and abnormal conditions.

4. Applicability:

4.1. Functional Entities:

4.1.1 Balancing Authority

4.1.1.1 The Balancing Authority is the responsible entity unless the Balancing Authority is a member of a Reserve Sharing Group, in which case, the Reserve Sharing Group becomes the responsible entity.

4.1.2 Reserve Sharing Group

4.1.2.1 The Reserve Sharing Group when comprised of a Source Balancing Authority becomes the source Reserve Sharing Group.

4.1.2.2 The Reserve Sharing Group when comprised of a Sink Balancing Authority becomes the sink Reserve Sharing Group.

5. Effective Date*: Immediately upon receipt of regulatory approval.

B. Requirements and Measures

R1. Each Balancing Authority and each Reserve Sharing Group shall maintain a minimum amount of Contingency Reserve, except within the first sixty minutes following an event requiring the activation of Contingency Reserve, that is*: [Violation Risk Factor: High] [Time Horizon: Real-time operations]*

1.1. The greater of either:

- The amount of Contingency Reserve equal to the loss of the most severe single contingency;
- The amount of Contingency Reserve equal to the sum of three percent of hourly integrated Load plus three percent of hourly integrated generation.

1.2. Composed of any combination of the reserve types specified below:

- Operating Reserve—Spinning
- Operating Reserve—Supplemental
- Interchange Transactions designated by the Source Balancing Authority as Operating Reserve—Supplemental

- Reserve held by other entities by agreement that is deliverable on Firm Transmission Service
- A resource, other than generation or load, that can provide energy or reduce energy consumption
- Load, including demand response resources, Demand-Side Management resources, Direct Control Load Management, Interruptible Load or Interruptible Demand, or any other Load made available for curtailment by the Balancing Authority or the Reserve Sharing Group via contract or agreement.
- All other load, not identified above, once the Reliability Coordinator has declared an energy emergency alert signifying that firm load interruption is imminent or in progress.

1.3. Based on real-time hourly load and generating energy values averaged over each Clock Hour (excluding Qualifying Facilities covered in 18 C.F.R.§ 292.101, as addressed in FERC Order 464).

1.4. An amount of capacity from a resource that is deployable within ten minutes.

M1. Each Balancing Authority and each Reserve Sharing Group will have documentation demonstrating its Contingency Reserve was maintained, except within the first sixty minutes following an event requiring the activation of Contingency Reserve.

Part 1.1

Each Balancing Authority and each Reserve Sharing Group will have dated documentation that demonstrates its Contingency Reserve was maintained in accordance with the amounts identified in Requirement R1, Part 1.1, except within the first sixty minutes following an event requiring the activation of Contingency Reserve.

Attachment A is a practical illustration showing how the generation amount may be calculated under Requirement R1.

- Where Dynamic Schedules are used as part of the generation amount upon which Contingency Reserve is predicated, additional evidence of compliance with Requirement R1, Part 1.1 may include, but is not limited to, documentation showing a reciprocal acknowledgement as to which entity is carrying the reserves. This transfer may be all or some portion of the physical generator and is not limited to the entire physical capability of the generator.
- Where Pseudo-Ties are used as part of the generation amount upon which Contingency Reserve is predicated, additional evidence of compliance with Requirement R1, Part 1.1, may include, but is not limited to, documentation accounting for the transfers included in the Pseudo-Ties.

Part 1.2

Each Balancing Authority and each Reserve Sharing Group will have dated documentation that demonstrates compliance with Requirement R1, Part 1.2.

Evidence may include, but is not limited to, documentation that reserves were comprised of the types listed in Requirement R1, Part 1.2 for purposes of meeting the Contingency Reserve obligation of Requirement R1. Additionally, for purposes of the last bullet of Requirement R1, Part 1.2, evidence of compliance may include, but is not limited to, documentation that the reliability coordinator had issued an energy emergency alert, indicating that firm Load interruption was imminent or was in progress.

Part 1.3

Each Balancing Authority and each Reserve Sharing Group will have dated documentation that demonstrates compliance with Requirement R1, Part 1.3. Evidence of compliance with Requirement R1, Part 1.3 may include, but is not limited to, documentation that Contingency Reserve amounts are based upon load and generating data averaged over each Clock Hour and excludes Qualifying Facilities covered in 18 C.F.R.§ 292.101, as addressed in FERC Order 464.

Part 1.4

Evidence of compliance with Requirement R1, Part 1.4 may include, but is not limited to, documentation that the reserves maintained to comply with Requirement R1, Part 1.4 are fully deployable within ten minutes.

R2. Reserved.

M2. Reserved.

R3. Each Sink Balancing Authority and each sink Reserve Sharing Group shall maintain an amount of Operating Reserve, in addition to the minimum Contingency Reserve in Requirement R1, equal to the amount of Operating Reserve–Supplemental for any Interchange Transaction designated as part of the Source Balancing Authority's Operating Reserve–Supplemental or source Reserve Sharing Group's Operating Reserve–Supplemental, except within the first sixty minutes following an event requiring the activation of Contingency Reserve. [*Violation Risk Factor: High] [Time Horizon: Real-time operations]*

M3. Each Sink Balancing Authority and each sink Reserve Sharing Group will have dated documentation demonstrating it maintained an amount of Operating Reserve, in addition to the Contingency Reserve identified in Requirement R1, equal to the amount of Operating Reserve–Supplemental for any Interchange Transaction designated as part of the Source Balancing Authority's Operating Reserve–Supplemental or source Reserve Sharing Group's Operating Reserve–Supplemental, for the entire period of the transaction, except within the first sixty minutes following an event requiring the activation of Contingency Reserves, in accordance with Requirement 3.

R4. Each Source Balancing Authority and each source Reserve Sharing Group shall maintain an amount of Operating Reserve, in addition to the minimum Contingency Reserve amounts identified in Requirement R1, equal to the amount and type of

Operating Reserves for any Operating Reserve transactions for which it is the Source Balancing Authority or source Reserve Sharing Group. *[Violation Risk Factor: High] [Time Horizon: Real-time operations]*

M4. Each Source Balancing Authority and each source Reserve Sharing Group will have dated documentation that demonstrates it maintained an amount of additional Operating Reserves identified in Requirement R1, greater than or equal to the amount and type of that identified in Requirement 4, for the entire period of the transaction.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The British Columbia Utilities Commission.

1.2. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot-Checking

Compliance Investigation

Self-Reporting

Complaint

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 Balancing Authority and each Reserve Sharing Group shall keep evidence for Requirement R1 through R4 for three years plus calendar current.

1.4. Additional Compliance Information:

1.4.1 This Standard shall apply to each Balancing Authority and each Reserve Sharing Group that has registered with WECC as provided in Part 1.4.2 of Section C.

Each Balancing Authority identified in the registration with WECC as provided in Part 1.4.2 of Section C shall be responsible for compliance with this Standard through its participation in the Reserve Sharing Group and not on an individual basis.

1.4.2 A Reserve Sharing Group may register as the Responsible Entity for purposes of compliance with this Standard by providing written notice to the WECC: 1) indicating that the Reserve Sharing Group is registering as the Responsible Entity for purposes of compliance with this Standard, 2) identifying each Balancing Authority that is a member of the Reserve Sharing Group, and 3) identifying the person or organization that will serve as agent on behalf of the Reserve Sharing Group for purposes of communications and data submissions related to or required by this Standard.

1.4.3 If an agent properly designated in accordance with Part 1.4.2 of Section C identifies individual Balancing Authorities within the Reserve Sharing Group responsible for noncompliance at the time of data submission, together with the percentage of responsibility attributable to each identified Balancing Authority, then, except as may otherwise be finally determined through a duly conducted review or appeal of the initial finding of noncompliance: 1) any penalties assessed for noncompliance by the Reserve Sharing Group shall be allocated to the individual Balancing Authorities identified in the applicable data submission in proportion to their respective percentages of responsibility as specified in the data submission, 2) each Balancing Authority shall be solely responsible for all penalties allocated to it according to its percentage of responsibility as provided in subsection 1) of this Part 1.4.3 of Section C, and 3) neither the Reserve Sharing Group nor any member of the Reserve Sharing Group shall be responsible for any portion of a penalty assessed against another member of the Reserve Sharing Group in accordance with subsection 1) of this Part 1.4.3 of Section C (even if the member of Reserve Sharing Group against which the penalty is assessed is not subject to or otherwise fails to pay its allocated share of the penalty).

1.4.4 If an agent properly designated in accordance with Part 1.4.2 of Section C fails to identify individual Balancing Authorities within the Reserve Sharing Group responsible for noncompliance at the time of data submission or fails to specify percentages of responsibility attributable to each identified Balancing Authority, any penalties for noncompliance shall be assessed against the agent on behalf of the Reserve Sharing Group, and it shall be the responsibility of the members of the Reserve Sharing Group to allocate responsibility for such noncompliance.

1.4.5 Any Balancing Authority that is a member of a Reserve Sharing Group that has failed to register as provided in Part 1.4.2 of Section C shall be subject to this Standard on an individual basis.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Balancing Authority or the Reserve Sharing Group that incurs one Clock Hour, during a calendar month, in which Contingency Reserve is less than 100% but greater than or equal to 90% of the required Contingency Reserve amount, with the characteristics specified in Requirement R1.	The Balancing Authority or the Reserve Sharing Group that incurs one Clock Hour, during a calendar month, in which Contingency Reserve is less than 90% but greater than or equal to 80% of the required Contingency Reserve amount, with the characteristics specified in Requirement R1.	The Balancing Authority or the Reserve Sharing Group that incurs one Clock Hour, during a calendar month, in which Contingency Reserve is less than 80% but greater than or equal to 70% of the required Contingency Reserve amount, with the characteristics specified in Requirement R1.	The Balancing Authority or the Reserve Sharing Group that incurs one Clock Hour, during a calendar month, in which Contingency Reserve is less than 70% of the required Contingency Reserve amount, with the characteristics specified in Requirement R1.
R2.	Reserved.			
R3.	The Balancing Authority or the Reserve Sharing Group that incurs one hour, during a calendar month, in which Contingency Reserve is less than 100% but greater than or equal to 90% of the required Operating Reserve amount specified in Requirement R3.	The Balancing Authority or the Reserve Sharing Group that incurs one hour, during a calendar month, in which Contingency Reserve is less than 90% but greater than or equal to 80% of the required Operating Reserve amount specified in Requirement R3.	The Balancing Authority or the Reserve Sharing Group that incurs one hour, during a calendar month, in which Contingency Reserve is less than 80% but greater than or equal to 70% of the required Operating Reserve amount specified in Requirement R3.	The Balancing Authority or the Reserve Sharing Group that incurs one hour, during a calendar month, in which Contingency Reserve is less than 70% of the required Operating Reserve amount specified in Requirement R3.
R4.	The Balancing Authority or the Reserve Sharing Group	The Balancing Authority or the Reserve Sharing Group	The Balancing Authority or the Reserve Sharing Group	The Balancing Authority or the Reserve Sharing Group

	that incurs one hour, during a calendar month, in which Contingency Reserve Operating Reserve is less than 100% but greater than or equal to 90% of the required Operating Reserve amount specified in Requirement R4.	that incurs one hour, during a calendar month, in which Contingency Reserve Operating Reserve is less than 90% but greater than or equal to 80% of the required Operating Reserve amount specified in Requirement R4.	that incurs one hour, during a calendar month, in which Contingency Reserve Operating Reserve is less than 80% but greater than or equal to 70% of the required Operating Reserve amount specified in Requirement R4.	that incurs one hour, during a calendar month, in which Contingency Reserve Operating Reserve is less than 70% of the required Operating Reserve amount specified in Requirement R4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	October 29, 2008	Adopted by NERC Board of Trustees	
1	October 21, 2010	Order issued remanding BAL-002-WECC-1	
2	November 7, 2012	Adopted by NERC Board of Trustees	
2	November 21, 2013	FERC Order issued approving BAL-002-WECC-2. (Order becomes effective 1/28/14.)	
2a	December 1, 2015	Approved by WECC Board of Directors	Clarified resources available for use in Requirement R2
2a	January 24, 2017	FERC approved	The Interpretation provides clarification regarding the types of resources that may be used to satisfy Contingency Reserve.
3	August 15, 2019	Adopted by the NERC Board of Trustees	The Interpretation was removed. Requirement R2 was deleted. Template and formatting were updated. Syntax and verb tense in Guideline section were corrected.

Standard Attachments

Attachment A

Attachment A is illustrative only; it is not a requirement. Requirement R1 calls for an amount of Contingency Reserve to be maintained, predicated on an amount of generation and load required in Requirement R1, Part 1.1., specifically:

"**1.1** The greater of either:

- The amount of Contingency Reserve equal to the loss of the most severe single contingency;
- The amount of Contingency Reserve equal to the sum of three percent of hourly integrated Load plus three percent of hourly integrated generation."

Attachment A illustrates one possible way to account for and calculate the amount of generation upon which the Contingency Reserve amount is predicated.

Below is a practical illustration showing how the generation amount may be calculated under Requirement R1 for Balancing Authorities (BA) and Reserve Sharing Groups (RSG).

BA1 / RSG 1	**Generation**	**Part of Generator**
Generator 1	300 MWs online	Yes
Generator 2	200 MWs online	Yes
Generator 3 (Pseudo-Tied out to BA2)	100 MWs online	No
Generator 4 QF (has backup contract)	10 MWs online	No
Generator 5 QF in EMS	10 MWs online	Yes
Generator 6	0 MWs online	Yes
Dynamic Schedule to BA2 from BA1[1]	(50 MWs)	
Generation	620 MWs	(The sum of gen 1–6)
BA generation (EMS)	510 MWs	(The sum of gen 1, 2, and 5)
Generation to use Under BAL-002-WECC-1	460 MWs**	(The sum of gen 1, 2, and 5 minus Dynamic Schedule)

** Assumes BA1 and BA2 agree on Dynamic Schedule treatment. If no agreement, BA1 would maintain reserves based on 510 MWs Generation.

BA2 / RSG2	**Generation**	**Part of Generator**
Generator 11	100 MWs	Yes
Generator 12	100 MWs	Yes
Generator 3 (Pseudo-Tied in from BA1)	100 MWs	Yes
Dynamic Schedule from BA1 to BA2	50 MWs	Yes
Generation	300 MWs	(The sum of gen 11, 12 and 3.)
BA generation (EMS)	300 MWs	(The sum of gen 11, 12 and 3)

[1] Note: This Dynamic Schedule is not the same as the Generator 3 Pseudo-Tie.

Generation to use Under BAL-002-WECC-1	350 MWs**	(The sum of gen 11, 12 and 3 plus Dynamic Schedule)

** Assumes BA1 and BA2 agree on Dynamic Schedule treatment. If no agreement, BA1 would have to maintain reserves based on 510MWs Generation and BA2 would determine its generation to be 300 MWs.

Guideline and Technical Basis

A Guidance Document addressing implementation of this standard was filed with Version 2.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

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 identification and categorization processes.

5. Effective Date*: See BC Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
The British Columbia Utilities Commission.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	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-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).	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-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).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	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 Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

- BC Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised

7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	3/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022

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 BC 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.
- **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.
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS;	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to:

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA		• 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.
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:	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	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. EACMS; 2. PACS; and 3. PCA	required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	
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	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		used to account for any differences in operation between the test and production environments.	
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:
The British Columbia Utilities Commission.

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) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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 configuration but did not verify and document that the required controls were

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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) OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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 performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	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)	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)	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)	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 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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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 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	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity failed to document or implement one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-4, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-4, 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-010-4,	Removable Media, but failed to implement the Removable Media sections according to CIP-010-4, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, 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-010-4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-4, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, 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-010-4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-4, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R4, Attachment 1, Section 1.2. (R4)	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-010-4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	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-010-4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

- BC Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
4	3/18/2021	FERC order approving Docket No. RD21-2-000	
4	4/5/2021	Effective Date	10/1/2022

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.

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 BC Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). 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 vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The British Columbia Utilities Commission.

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- BC Implementation Plan for Project 2019-03
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	
2	3/18/2021	FERC Order approving CIP-013-2.Docket No. RD21-2-000.	
2	4/5/2021	Effective Date	10/1/2022

A. Introduction

1. **Title:** **Emergency Preparedness and Operations**

2. **Number:** **EOP-011-2**

3. **Purpose:** To address the effects of operating emergencies by ensuring each Transmission Operator, Balancing Authority, and Generator Owner has developed plan(s) to mitigate operating Emergencies and that those plans are implemented and coordinated within the Reliability Coordinator Area as specified within the requirements.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Reliability Coordinator

   4.1.3 Transmission Operator

   3.1.4 Generator Owner

   3.1.5 Generator Operator

   4.2. Facilities

   4.2.1 For the purpose of this standard, the term "generating unit" means all Bulk Electric System generators.

5. **Effective Date*:** See BC Implementation Plan for Project 2019-06.

B. Requirements and Measures

R1. Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

1.1. Roles and responsibilities for activating the Operating Plan(s);

1.2. Processes to prepare for and mitigate Emergencies including:

1.2.1. Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;

1.2.2. Cancellation or recall of Transmission and generation outages;

1.2.3. Transmission system reconfiguration;

1.2.4. Redispatch of generation request;

1.2.5. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

1.2.6. Provisions to determine reliability impacts of:

1.2.6.1. cold weather conditions; and

1.2.6.2. extreme weather conditions.

M1. Each Transmission Operator will have a dated Operating Plan(s) developed in accordance with Requirement R1 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R1.

R2. Each Balancing Authority shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate Capacity Emergencies and Energy Emergencies within its Balancing Authority Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

2.1. Roles and responsibilities for activating the Operating Plan(s);

2.2. Processes to prepare for and mitigate Emergencies including:

2.2.1. Notification to its Reliability Coordinator, to include current and projected conditions when experiencing a Capacity Emergency or Energy Emergency;

2.2.2. Requesting an Energy Emergency Alert, per Attachment 1;

2.2.3. Managing generating resources in its Balancing Authority Area to address:

2.2.3.1. capability and availability;

2.2.3.2. fuel supply and inventory concerns;

2.2.3.3. fuel switching capabilities; and

2.2.3.4. environmental constraints.

2.2.4. Public appeals for voluntary Load reductions;

2.2.5. Requests to government agencies to implement their programs to achieve necessary energy reductions;

2.2.6. Reduction of internal utility energy use;

2.2.7. Use of Interruptible Load, curtailable Load and demand response;

2.2.8. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

2.2.9. Provisions to determine reliability impacts of:

2.2.9.1. cold weather conditions; and

2.2.9.2. extreme weather conditions.

M2. Each Balancing Authority will have a dated Operating Plan(s) developed in accordance with Requirement R2 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R2.

R3. The Reliability Coordinator shall review the Operating Plan(s) to mitigate operating Emergencies submitted by a Transmission Operator or a Balancing Authority regarding any reliability risks that are identified between Operating Plans. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

3.1. Within 30 calendar days of receipt, the Reliability Coordinator shall:

3.1.1. Review each submitted Operating Plan(s) on the basis of compatibility and inter-dependency with other Balancing Authorities' and Transmission Operators' Operating Plans;

3.1.2. Review each submitted Operating Plan(s) for coordination to avoid risk to Wide Area reliability; and

3.1.3. Notify each Balancing Authority and Transmission Operator of the results of its review, specifying any time frame for resubmittal of its Operating Plan(s) if revisions are identified.

M3. The Reliability Coordinator will have documentation, such as dated e-mails or other correspondences that it reviewed Transmission Operator and Balancing Authority Operating Plans within 30 calendar days of submittal in accordance with Requirement R3.

R4. Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator. *[Violation Risk Factor: High] [Time Horizon: Operation Planning]*

M4. The Transmission Operator and Balancing Authority will have documentation, such as dated emails or other correspondence, with an Operating Plan(s) version history showing that it responded and updated the Operating Plan(s) within the timeframe identified by its Reliability Coordinator in accordance with Requirement R4.

R5. Each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority within its Reliability Coordinator Area shall notify, within 30 minutes from the time of receiving notification, other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and

neighboring Reliability Coordinators. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M5. Each Reliability Coordinator that receives an Emergency notification from a Balancing Authority or Transmission Operator within its Reliability Coordinator Area will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that will be used to determine if the Reliability Coordinator communicated, in accordance with Requirement R5, with other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators .

R6. Each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall declare an Energy Emergency Alert, as detailed in Attachment 1. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M6. Each Reliability Coordinator, with a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area, will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that it declared an Energy Emergency Alert, as detailed in Attachment 1, in accordance with Requirement R6.

R7. Each Generator Owner shall implement and maintain one or more cold weather preparedness plan(s) for its generating units. The cold weather preparedness plan(s) shall include the following, at a minimum: [*Violation Risk Factor: High*] [*Time Horizon: Operations Planning and Real-Time Operations*]

7.1. Generating unit(s) freeze protection measures based on geographical location and plant configuration;

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

7.3. Generating unit(s) cold weather data, to include:

7.3.1. Generating unit(s) operating limitations in cold weather to include:

7.3.1.1. capability and availability;

7.3.1.2. fuel supply and inventory concerns;

7.3.1.3. fuel switching capabilities; and

7.3.1.4. environmental constraints.

7.3.2. Generating unit(s) minimum:

7.3.2.1. design temperature; or

7.3.2.2. historical operating temperature; or

7.3.1.3. current cold weather performance temperature determined by an engineering analysis.

M7. Each Generator Owner will have evidence documenting that its cold weather preparedness plan(s) was implemented and maintained in accordance with Requirement R7.

R8. Each Generator Owner in conjunction with its Generator Operator shall identify the entity responsible for providing the generating unit-specific training, and that identified entity shall provide the training to its maintenance or operations personnel responsible for implementing cold weather preparedness plan(s) developed pursuant to Requirement R7. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning, Operations Planning]*

M8. Each Generator Operator or Generator Owner will have documented evidence that the applicable personnel completed training of the Generator Owner's cold weather preparedness plan(s). This evidence may include, but is not limited to, documents such as personnel training records, training materials, date of training, agendas or learning objectives, attendance at pre-work briefings, review of work order tasks, tailboards, attendance logs for classroom training, and completion records for computer-based training in fulfillment of Requirement R8.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The British Columbia Utilities Commission.

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 Transmission Operator shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R1 and R4 and Measures M1 and M4.
- The Balancing Authority shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R2 and R4, and Measures M2 and M4.
- The Reliability Coordinator shall maintain evidence of compliance since the

last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.

- The Generator Owner shall retain the cold weather preparedness plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirement R7 and Measure M7.

1.3. The Generator Owner or Generator Operator shall keep data or evidence to show compliance for three years or since its last compliance audit, whichever timeframe is greater, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation, for Requirement R8 and Measure M8.

1.4. 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 #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to maintain it.	The Transmission Operator developed an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to have it reviewed by its Reliability Coordinator.	The Transmission Operator failed to develop an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. OR The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission s Operator Area but failed to implement it.
R2	Real-time Operations, Operations	High	N/A	The Balancing Authority developed a Reliability Coordinator-	The Balancing Authority developed an Operating Plan(s) to mitigate operating	The Balancing Authority failed to develop an

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning, Long-term Planning			reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to maintain it.	Emergencies within its Balancing Authority Area but failed to have it reviewed by its Reliability Coordinator.	Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area. OR The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to implement it.
R3	Operations Planning	High	N/A	N/A	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Operator within 30 calendar days.	
R4	Operations Planning	High	N/A	N/A	The Transmission Operator or Balancing Authority failed to update and resubmit tis Operating Plan(s) to its Reliability Coordinator within the timeframe specified by its Reliability Coordinator.	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator.
R5	Real-time Operations	High	N/A	N/A	The Reliability Coordinator that received an Emergency notification from a Transmission Operator or Balancing Authority did notify neighboring Reliability Coordinators, Balancing Authorities	The Reliability Coordinator that received an Emergency notification from a Transmission Operator or Balancing Authority failed to notify neighboring Reliability Coordinators, Balancing Authorities

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					and Transmission Operators but failed to notify within 30 minutes from the time of receiving notification.	and Transmission Operators.
R6	Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator that had a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area failed to declare an Energy Emergency Alert.
R7	Operations Planning and Real-time Operations	High	The Generator Owner implemented a cold weather preparedness plan(s) but failed to maintain it.	The Generator Owner's cold weather preparedness plan failed to include one of the applicable requirement Parts within Requirement R7.	The Generator Owner had and maintained a cold weather preparedness plan(s) but failed to fully implement it. OR	The Generator Owner does not have a cold weather preparedness plan. OR The Generator Owner has a cold

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Generator Owner's cold weather preparedness plan failed to include two of the applicable requirement Parts within Requirement R7.	weather preparedness plan, but failed to include any of the applicable requirement Parts within Requirement R7.
R8	Operations Planning and Real-time Operations	Medium	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • one applicable personnel at a single generating unit; or • 5% or less of its total applicable personnel.	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • two applicable personnel at a single generating unit; or • more than 5% or less than or equal to 10% of its total applicable personnel.	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • three applicable personnel at a single generating unit; or • more than 10% or less than or equal to 15% of its total applicable personnel.	The Generator Owner or Generator Operator failed to provide generating unit-specific training as described in Requirement R8 to the greater of: • four applicable personnel at a single generating unit; or • more than 15% of its total applicable personnel.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

BC Implementation Plan for Project 2019-06.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by Board of Trustees	Merged EOP-001-2.1b, EOP-002-3.1 and EOP-003-2.
1	November 19, 2015	FERC approved EOP-011-1. Docket Nos. RM15-7-000, RM15-12-000, and RM15-13-000. Order No. 818	
2	June 11,2021	Adopted by the Board of Trustees	Revised under Project 2019-06
2	August 24,2021	FERC approved EOP-011-2. Docket Number RD21-5-000	
2	August 24,2021	Effective Date	4/1/ 2023

Attachment 1-EOP-011-2
Energy Emergency Alerts

Introduction

This Attachment provides the process and descriptions of the levels used by the Reliability Coordinator in which it communicates the condition of a Balancing Authority which is experiencing an Energy Emergency.

A. General Responsibilities

1. **Initiation by Reliability Coordinator.** An Energy Emergency Alert (EEA) may be initiated only by a Reliability Coordinator at 1) the Reliability Coordinator's own request, or 2) upon the request of an energy deficient Balancing Authority.

2. **Notification**. A Reliability Coordinator who declares an EEA shall notify all Balancing Authorities and Transmission Operators in its Reliability Coordinator Area. The Reliability Coordinator shall also notify all neighboring Reliability Coordinators.

B. EEA Levels

Introduction

To ensure that all Reliability Coordinators clearly understand potential and actual Energy Emergencies in the Interconnection, NERC has established three levels of EEAs. The Reliability Coordinators will use these terms when communicating Energy Emergencies to each other. An EEA is an Emergency procedure, not a daily operating practice, and is not intended as an alternative to compliance with NERC Reliability Standards.

The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially.

1. **EEA 1 — All available generation resources in use.**

Circumstances:

- The Balancing Authority is experiencing conditions where all available generation resources are committed to meet firm Load, firm transactions, and reserve commitments, and is concerned about sustaining its required Contingency Reserves.
- Non-firm wholesale energy sales (other than those that are recallable to meet reserve requirements) have been curtailed.

2. **EEA 2 — Load management procedures in effect**.

Circumstances:

- The Balancing Authority is no longer able to provide its expected energy requirements and is an energy deficient Balancing Authority.
- An energy deficient Balancing Authority has implemented its Operating Plan(s) to mitigate Emergencies.

- An energy deficient Balancing Authority is still able to maintain minimum Contingency Reserve requirements.

During EEA 2, Reliability Coordinators and energy deficient Balancing Authorities have the following responsibilities:

2.1 Notifying other Balancing Authorities **and market participants**. The energy deficient Balancing Authority shall communicate its needs to other Balancing Authorities and market participants. Upon request from the energy deficient Balancing Authority, the respective Reliability Coordinator shall post the declaration of the alert level, along with the name of the energy deficient Balancing Authority on the RCIS website.

2.2 Declaration period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 2 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators**.**

2.3 Sharing information on resource availability. Other Reliability Coordinators of Balancing Authorities with available resources shall coordinate, as appropriate, with the Reliability Coordinator that has an energy deficient Balancing Authority.

2.4 Evaluating and mitigating Transmission limitations. The Reliability Coordinator shall review Transmission outages and work with the Transmission Operator(s) to see if it's possible to return to service any Transmission Elements that may relieve the loading on System Operating Limits (SOLs) or Interconnection Reliability Operating Limits (IROLs).

2.5 Requesting Balancing Authority actions. Before requesting an EEA 3, the energy deficient Balancing Authority must make use of all available resources; this includes, but is not limited to:

2.5.1 All available generation units are on line. All generation capable of being on line in the time frame of the Emergency is on line.

2.5.2 Demand-Side Management. Activate Demand-Side Management within provisions of any applicable agreements.

3. EEA 3 —Firm Load interruption is imminent or in progress.

Circumstances:

- The energy deficient Balancing Authority is unable to meet minimum Contingency Reserve requirements.

During EEA 3, Reliability Coordinators and Balancing Authorities have the following responsibilities:

3.1 Continue actions from EEA 2. The Reliability Coordinators and the energy deficient Balancing Authority shall continue to take all actions initiated during EEA 2.

3.2 Declaration Period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 3 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities, and Transmission Operators.

3.3 Reevaluating and revising SOLs and IROLs. The Reliability Coordinator shall evaluate the risks of revising SOLs and IROLs for the possibility of delivery of energy to the energy deficient Balancing Authority. Reevaluation of SOLs and IROLs shall be coordinated with other Reliability Coordinators and only with the agreement of the Transmission Operator whose Transmission Owner (TO) equipment would be affected. SOLs and IROLs shall only be revised as long as an EEA 3 condition exists, or as allowed by the Transmission Owner whose equipment is at risk. The following are minimum requirements that must be met before SOLs or IROLs are revised:

3.3.1 Energy deficient Balancing Authority obligations. The energy deficient Balancing Authority, upon notification from its Reliability Coordinator of the situation, it will immediately take whatever actions are necessary to mitigate any undue risk to the Interconnection. These actions may include Load shedding.

3.4 Returning to pre-Emergency conditions. Whenever energy is made available to an energy deficient Balancing Authority such that the Systems can be returned to its pre-Emergency SOLs or IROLs condition, the energy deficient Balancing Authority shall request the Reliability Coordinator to downgrade the alert level.

3.4.1 Notification of other parties. Upon notification from the energy deficient Balancing Authority that an alert has been downgraded, the Reliability Coordinator shall notify the neighboring Reliability Coordinators (via the RCIS), Balancing Authorities and Transmission Operators that its Systems can be returned to its normal limits.

Alert 0 - Termination. When the energy deficient Balancing Authority is able to meet its Load and Operating Reserve requirements, it shall request its Reliability Coordinator to terminate the EEA**.**

3.4.2 Notification. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS of the termination. The Reliability Coordinator shall also notify the neighboring Balancing Authorities and Transmission Operators.

A. Introduction

1. **Title:** Facility Ratings

2. **Number:** FAC-008-5

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.

4. **Applicability:**

   4.1. Transmission Owner

   4.2. Generator Owner

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

B. Requirements and Measures

R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:

- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
- Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

M1. Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.

R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:

2.2.1. Equipment Rating standard(s) used in development of this methodology.

2.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

2.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

2.2.4. Operating limitations.[1]

2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.4. The process by which the Rating of equipment that comprises a Facility is determined.

2.4.1. The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

2.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

M2. Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.

R3. Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

[1] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

3.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:

3.2.1. Equipment Rating standard(s) used in development of this methodology.

3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

3.2.4. Operating limitations.[2]

3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

3.4. The process by which the Rating of equipment that comprises a Facility is determined.

3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

M3. Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.

R4. Reserved.

M4. Reserved.

R5. Reserved.

M5. Reserved.

R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).

R7. Reserved.

M7. Reserved.

[2] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

8.1. As scheduled by the requesting entities:

8.1.1. Facility Ratings

8.1.2. Identity of the most limiting equipment of the Facilities

8.2. Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1. Identity of the existing next most limiting equipment of the Facility

8.2.2. The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

M8. Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
The British Columbia Utilities Commission.

1.2. Compliance Monitoring and Enforcement Processes:

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting

- Compliance Violation Investigations
- Complaints

1.3. 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 Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.
- The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.
- The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.
- The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.
- The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.
- If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.
- The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. 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 Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2.	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part 2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2 OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
R4. Reserved.				
R5. Reserved.				

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
R7. Reserved.				
R8.	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%,	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)	not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)	requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from "Lower" to "Medium"	
3	February 7, 2013	R4 and 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.	
3	November 21, 2013	R4 and R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
4	May 9, 2020	R7 and R8 and associated elements adopted by NERC Board of Trustees for retirement as part of Project 2018-03 Standards Efficiency Review Retirements.	
4	September 17, 2020	Remanded by FERC (Order No. 873).	Withdrawn
5	February 4, 2021	Adopted by NERC Board of Trustees	Requirement R8 and associated elements restored in response

Version	Date	Action	Change Tracking
			to FERC Order No. 873.
5	April 7,2021	FERC Order approving FAC-008-5. Docket No. RD21-4-000	
5	October 1,2021	Effective Date	

A. Introduction

1. **Title:** Evaluation of Interchange Transactions
2. **Number:** INT-006-5
3. **Purpose:** To ensure that responsible entities conduct a reliability assessment of each Arranged Interchange before it is implemented.
4. **Applicability:**
   - **4.1.** Balancing Authority
   - **4.2.** Transmission Service Provider
5. **Effective Date*:** See Implementation Plan.

B. Requirements and Measures

R1. Each Balancing Authority shall approve or deny each on-time Arranged Interchange or emergency Arranged Interchange that it receives and shall do so prior to the expiration of the time period defined in Attachment 1, Column B. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

1.1. Each Source and Sink Balancing Authority shall deny the Arranged Interchange or curtail Confirmed Interchange if it does not expect to be capable of supporting the magnitude of the Interchange, including ramping, throughout the duration of the Arranged Interchange.

1.2. Each Balancing Authority shall deny the Arranged Interchange or curtail Confirmed Interchange if the Scheduling Path (proper connectivity of Adjacent Balancing Authorities) between it and its Adjacent Balancing Authorities is invalid.

M1. Each Balancing Authority shall have evidence (such as dated and time stamped electronic logs, or other evidence) that it responded to each request for its approval to transition an Arranged Interchange to a Confirmed Interchange within the time defined in Attachment 1, Column B. (R1)

R2. Each Transmission Service Provider shall approve or deny each on-time Arranged Interchange or emergency Arranged Interchange that it receives and shall do so prior to the expiration of the time period defined in Attachment 1, Column B. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

2.1. Each Transmission Service Provider shall deny the Arranged Interchange or curtail Confirmed Interchange if the transmission path (proper connectivity of adjacent Transmission Service Providers) between it and its adjacent Transmission Service Providers is invalid.

M2. Each Transmission Service Provider shall have evidence (such as dated and time stamped electronic logs, studies, or other evidence) that it responded to each Arranged Interchange or emergency Arranged Interchange within the time defined in Attachment 1, Column B. If the transmission path between the Transmission Service Provider and its adjacent Transmission Service Providers is invalid, each Transmission Service Provider shall have evidence (such as dated and time stamped electronic logs, studies, or other evidence) that it denied the Arranged Interchange or curtailed confirmed Interchange. (R2)

R3. The Source Balancing Authority and the Sink Balancing Authority receiving a Reliability Adjustment Arranged Interchange shall approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning, Same-day Operations, Real-time Operations]*

M3. Each Balancing Authority shall have evidence (such as dated and time stamped electronic logs, studies, or other evidence) that when responding to a Reliability Adjustment Arranged Interchange, it either approved the request or denied the request.

R4. Reserved.

M4. Reserved.

R5. Reserved.

M5. Reserved.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
The British Columbia Utilities Commission

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 Balancing Authority shall maintain evidence to show compliance with R1 and R3 for the most recent three calendar months plus the current month.
- The Transmission Service Provider shall maintain evidence to show compliance with R2 for the most recent three calendar months plus the current month.
- If a Balancing Authority or Transmission Service Provider is found non-compliant, it shall keep information related to the non-compliance until found compliant.

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

1.3. Compliance Monitoring and 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.

- Compliance Audits

- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaint

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Operations Planning, Same-day Operations, Real-time Operations	Lower	N/A	N/A	N/A	The Balancing Authority receiving an on-time Arranged Interchange or an emergency Arranged Interchange did not approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B. OR The Source or Sink Balancing Authority did not expect to be capable of supporting the magnitude of the Interchange, including ramping, throughout duration of the Arranged Interchange and did not deny the Arranged Interchange or curtail Confirmed Interchange. OR The Scheduling Path between the Balancing

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Authority and its Adjacent Balancing Authorities was invalid, and the Balancing Authority did not deny the Arranged Interchange or curtail Confirmed Interchange.
R2.	Operations Planning, Same-day Operations, Real-time Operations	Lower	N/A	N/A	N/A	The Transmission Service Provider receiving an on-time Arranged Interchange or an emergency Arranged Interchange did not approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B. OR The transmission path between the Transmission Service Provider and its adjacent Transmission Service Providers was invalid, and the Transmission

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Service Provider did not deny the Arranged Interchange or curtail Confirmed Interchange.
R3.	Operations Planning, Same-day Operations, Real-time Operations	Lower	N/A	N/A	The Source Balancing Authority or Sink Balancing Authority receiving a Reliability Adjustment Arranged Interchange denied it prior to the expiration of the time period defined in Attachment 1, Column B.	The Source Balancing Authority or Sink Balancing Authority receiving a Reliability Adjustment Arranged Interchange did not approve or deny it prior to the expiration of the time period defined in Attachment 1, Column B.
R4. Reserved.						
R5. Reserved.						

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by the NERC Board Of Trustees	New
2	May 2, 2007	Adopted by the NERC Board Of Trustees	Revised
3	October 29, 2008	Adopted by the NERC Board Of Trustees	Revised
3	July 1, 2010	Approved by FERC	Revised
4	February 6, 2014	Adopted by the NERC Board Of Trustees	Revised
4	June 30, 2014	FERC letter order issued approving INT-006-4	
5	May 9, 2019	Adopted by the NERC Board of Trustees	Requirements R3.1, R4, and R5 retired under Project 2018-03 Standard Efficiency Review Retirements.
5	September 17, 2020	FERC Order issued approving INT-006-5. Docket No. RM19-16-000, RM19-17-000	
5	December 14,2020		FERC Approval
5	April 1, 2021	Effective Date	

Timing Tables

Timing Requirements for all Interconnections except WECC

		A	B	C	D
If Arranged Interchange [1] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange[2]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[2]**	**BA Prepares Confirmed Interchange for Implementation**
>1 hour after the start time	ATF		Entities have up to 2 hours to respond.		NA
<15 minutes prior to ramp start and ≤1 hour after the start time	Late		Entities have up to 10 minutes to respond.		≤ 3 minutes after receipt of Confirmed Interchange
<1 hour and ≥ 15 minutes prior to ramp start	On-time		≤ 10 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
≥1 hour to < 4 hours prior to ramp start	On-time		≤ 20 minutes from Arranged Interchange receipt		≥ 39 minutes prior to ramp start
≥ 4 hours prior to ramp start	On-time		≤ 2 hours from Arranged Interchange receipt		≥ 1 hour 58 minutes prior to ramp start

[1] Time Classifications and deadlines apply to both initial Arranged Interchange submittal and any subsequent modifications to the Arranged Interchange.
[2] See NAESB WEQ004. The times are being retained in the NAESB tables but are removed here since they are not being referenced in requirements.

Timing Tables

Timing Requirements for WECC

		A	B	C	D
If Arranged Interchange [3] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange[4]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[4]**	**BA Prepares Confirmed Interchange for Implementation**
>1 hour after the start time	ATF		Entities have up to 2 hours to respond.		NA
<10 minutes prior to ramp start and ≤1 hour after transaction start time where transaction start time is at the top of the hour	Late		Entities have up to 10 minutes to respond.		≤ 3 minutes after receipt of Confirmed Interchange
<15 minutes prior to ramp start and ≤1 hour after transaction start time where transaction start time is not the top of the hour	Late		Entities have up to 10 minutes to respond.		≤ 3 minutes after receipt of Confirmed Interchange

[3] Time Classifications and deadlines apply to both initial Arranged Interchange submittal and any subsequent modifications to the Arranged Interchange.
[4] See NAESB WEQ004. The times are being retained in the NAESB tables but are removed here since they are not being referenced in requirements.

		A	B	C	D
If Arranged Interchange [3] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange[4]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[4]**	**BA Prepares Confirmed Interchange for Implementation**
10 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 5 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
11 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 6 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
12 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 7 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
13 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 8 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start

		A	B	C	D
If Arranged Interchange [3] is Submitted	**Time Classification**	**Sink BA Makes Initial Distribution of Arranged Interchange[4]**	**BA and TSP Conduct Reliability Assessments**	**Compilation and Distribution Status[4]**	**BA Prepares Confirmed Interchange for Implementation**
14 minutes prior to ramp start where transaction start time is at the top of the hour	On-time		≤ 9 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
<1 hour and ≥ 15 minutes prior to ramp start	On-time		≤ 10 minutes from Arranged Interchange receipt		≥ 3 minutes prior to ramp start
≥ 1 hour and < 4 hours prior to ramp start	On-time		< 20 minutes from Arranged interchange receipt		≥ 39 minutes prior to ramp start
≥ 4 hours prior to ramp start	On-time		≤ 2 hours from Arranged Interchange receipt		≥ 1 hour 58 minutes prior to ramp start
Submitted before 10:00 PPT with start time ≥ 00:00 PPT of following day	On-time		By 12:00 PPT of day the Arranged Interchange was received		≥ 1 hour 58 minutes prior to ramp start

Guidelines and Technical Basis

Many aspects of managing Interchange are supported by software applications. There are fundamental tasks that each entity should be able to perform in an electronic manner as listed below.

A Load-Serving Entity and Balancing Authority that submits Requests for Interchange should have the capability to electronically:

- Submit a Request for Interchange to a Sink Balancing Authority
- Submit a request to modify Interchange
- Receive distributions of Confirmed Interchange
- Receive distributions of Reliability Adjustment Arranged Interchanges

Each Sink Balancing Authority should have the capability to electronically:

- Receive a Request for Interchange
- Receive a request to modify Interchange
- Validate Requests for Interchange by verifying:
    - Source Balancing Authority megawatts equal Sink Balancing Authority megawatts (adjusted for losses, if appropriate).
    - All reliability entities involved in the Arranged Interchange are valid.
    - Generation source and Load sink are defined.
    - Megawatt profile is defined.
    - Interchange duration is defined.
- Validate request to modify Interchange by verifying:
    - Source Balancing Authority megawatts equal Sink Balancing Authority megawatts (adjusted for losses, if appropriate).
    - Megawatt profile is defined.
    - Interchange duration is defined.
- Distribute the validated Request for Interchange as Arranged Interchange
- Distribute the validated Reliability Adjustment Arranged Interchanges
- Receive communication of approval or denial of Arranged Interchange
    - Distribute notification as each entity approves or denies an Arranged Interchange.
    - Transition Arranged Interchange to Confirmed Interchange if all approvals are received.
    - Distribute notification of whether Arranged Interchange was transitioned to Confirmed Interchange or not.

  - Submit a request to modify Interchange

- Each Load-Serving Entity that approves or denies Arranged Interchange, and each Balancing Authority and Transmission Service Provider should have the capability to electronically:
  - Receive distribution of Arranged Interchange
  - Communicate approval or denial of the Arranged Interchange to the Sink Balancing Authority
  - Receive notification of whether Arranged Interchange was transitioned to Confirmed interchange or not.
  - Submit a request to modify Interchange
- While Interchange is normally facilitated using electronic communication and software tools, there are occasions with those electronic capabilities are reduced or unavailable. It is recommended that all entities involved in aspects of Interchange should have, maintain and implement a plan describing the manner and timing in which all capabilities listed above will be provided when electronic capabilities are reduced or unavailable. Each plan should address the following topics:
  - Alternate methods of communicating Interchange information between Purchasing Selling Entities, Balancing Authorities, and Transmission Service Providers.
  - How to notify others that it is activating the plan
  - How it will process requests for emergency Arranged Interchange and Reliability Adjustment Arranged Interchange.
  - Restrictions and limitations that may apply during the period of reduced or unavailable capability (such as limits on volume, only accepting emergency transactions, etc.).
  - Delegation of approval rights and proxy actions, if such approaches will be used.
  - How known Confirmed Interchange will be scheduled following a reduction in or loss of capability.
  - Personnel plans for short-term and extended periods.
  - Training of personnel in the use of the plan.

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:

Balancing Authorities must take action on a received Arranged Interchange within a certain time frame. Requirement R1, Parts 1.1 and 1.2 provide reliability-related reasons that a Balancing Authority must deny an Arranged Interchange, but Balancing Authorities may deny

for other reasons. If the conditions described in Requirement R1, Parts 1.1 or 1.2 are recognized after approval is granted, the Balancing Authority may curtail the Confirmed Interchange prior to implementation.

Rationale for R2:
TSPs must take action on a received Arranged Interchange within a certain time frame. Requirement R2, Part 2.1 provides reliability-related reasons that a TSP must deny an Arranged Interchange, but TSPs may deny for other reasons. If the conditions described in Requirement R1, Part 2.1 are recognized after approval is granted, the TSP may curtail the Confirmed Interchange prior to implementation.

A. Introduction

1. **Title:** Implementation of Interchange

2. **Number:** INT-009-3

3. **Purpose:** To ensure that Balancing Authorities implement the Interchange as agreed upon in the Interchange confirmation process.

4. **Applicability:**

   4.1. Balancing Authority

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

B. Requirements and Measures

R1. Each Balancing Authority shall agree with each of its Adjacent Balancing Authorities that its Composite Confirmed Interchange with that Adjacent Balancing Authority, at mutually agreed upon time intervals, excluding Dynamic Schedules and Pseudo-Ties and including any Interchange not yet captured in the Composite Confirmed Interchange, is: [*Violation Risk Factor: Medium*] [*Time Horizon: Real-time Operations*]

1.1. Identical in magnitude to that of the Adjacent Balancing Authority, and

1.2. Opposite in sign or direction to that of the Adjacent Balancing Authority.

M1. The Balancing Authority shall have evidence (such as dated logs, voice recordings, electronic records, or other evidence) that its Composite Confirmed Interchange, excluding Dynamic Schedules and Pseudo-Ties and including any Interchange not yet captured in the Composite Confirmed Interchange, was agreed to by each Adjacent Balancing Authority, identical in magnitude to those of each Adjacent Balancing Authority, and opposite in sign to that of each Adjacent Balancing Authority. (R1)

R2. Reserved.

M2. Reserved.

R3. Each Balancing Authority in whose area the high-voltage direct current tie is controlled shall coordinate the Confirmed Interchange prior to its implementation with the Transmission Operator of the high-voltage direct current tie. [*Violation Risk Factor: Medium*] [*Time Horizon: Real-time Operations, Operations Planning*]

M3. The Balancing Authority shall have evidence (such as dated logs, electronic records, or other evidence) that it coordinated the Confirmed Interchange prior to its implementation with the Transmission Operator of the high-voltage direct current tie. (R3)

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
The British Columbia Utilities Commission.

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 Balancing Authority shall maintain evidence to show compliance with R1 and R3 for the most recent 3 months plus the current month.

If a Balancing Authority is found non-compliant, it shall keep information related to the non-compliance until found compliant.

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

1.3. Compliance Monitoring and 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.

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

Violation Severity Levels

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	The Balancing Authority did not reach agreement with an Adjacent Balancing Authority on the magnitude or sign of its Composite Confirmed Interchange, at mutually agreed upon time intervals, excluding Dynamic Schedules and Pseudo-Ties and including any Interchange not yet captured in the Composite Confirmed Interchange.
R2. Reserved.						
R3.	Real-time Operations, Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority failed to coordinate the Confirmed Interchange prior to its implementation with the Transmission Operator of the high-voltage direct current tie.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	May 2, 2006	Adopted by the NERC Board of Trustees	Revised
2	February 6, 2014	Adopted by the NERC Board of Trustees	Revised
2	June 30, 2014	FERC letter order issued approving INT-009-2	
2.1	August 22, 2014	Errata submitted for INT-004-3, INT-009-2, INT-010-2 and INT-011-2 to correct inconsistency between the Implementation Plan and the effective date language. The NERC Standards Committee approved errata changes on August 20, 2014.	Errata
2.1	November 26, 2014	FERC letter order approving errata changes.	
3	May 9, 2019	Adopted by NERC Board of Trustees	Requirement R2 retired under Project 2018-03 Standard Efficiency Review Retirements.
3	September 17, 2020	FERC Order issued approving INT-009-3. Docket No. RM19-16-000, RM19-17-000	
3	December 14,2020		FERC Approval

3	April 1, 2021	Effective Date	

A. Introduction

1. **Title:** Reliability Coordination – Monitoring and Analysis
2. **Number:** IRO-002-7
3. **Purpose:** To provide System Operators with the capabilities necessary to monitor and analyze data needed to perform their reliability functions.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Reliability Coordinators
5. **Effective Date*:** See Implementation Plan

B. Requirements and Measures

R1. Reserved.

M1. Reserved.

R2. Each Reliability Coordinator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing its Real-time monitoring and Real-time Assessments. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M2. Each Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, as specified in the requirement.

R3. Each Reliability Coordinator shall test its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Reliability Coordinator shall initiate action within two hours to restore redundant functionality. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Reliability Coordinator shall have, and provide upon request, evidence that it tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality, or experienced an event that demonstrated the redundant functionality; and if the test was unsuccessful, initiated action within two hours to restore redundant functionality as specified in Requirement R3. Evidence

could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, or electronic communications.

R4. Each Reliability Coordinator shall provide its System Operators with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M4. Each Reliability Coordinator shall have, and provide upon request evidence that could include, but is not limited to, a documented procedure or equivalent evidence that will be used to confirm that the Reliability Coordinator has provided its System Operators with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities.

R5. Each Reliability Coordinator shall monitor Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M5. Each Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, Energy Management System description documents, computer printouts, SCADA data collection, or other equivalent evidence that will be used to confirm that it has monitored Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area.

R6. Each Reliability Coordinator shall have monitoring systems that provide information utilized by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant infrastructure. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M6. The Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, Energy Management System description documents, computer printouts, SCADA data collection, or other equivalent evidence that will be used to confirm that it has monitoring systems consistent with the requirement.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The British Columbia Utilities Commission.

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 retain its current, in force document and any documents in force for the current year and previous calendar year for Requirements R2 and R4 and Measures M2 and M4.
- The Reliability Coordinator shall retain evidence for Requirement R3 and Measure M3 for the most recent 12 calendar months, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.
- The Reliability Coordinator shall keep data or evidence for Requirements R5 and R6 and Measures M5 and M6 for the current calendar year and one previous calendar year.

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. Reserved.				
R2.	N/A	N/A	The Reliability Coordinator had data exchange capabilities with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing Real-time monitoring and Real-time Assessments, but did not have redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center, as specified in the requirement.	The Reliability Coordinator did not have data exchange capabilities with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing Real-time monitoring and Real-time Assessments as specified in the requirement.
R3.	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for	The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	redundant functionality, but did so more than 90 calendar days but less than or equal to 120 calendar days since the previous test; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 2 hours and less than or equal to 4 hours.	redundant functionality, but did so more than 120 calendar days but less than or equal to 150 calendar days since the previous test; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 4 hours and less than or equal to 6 hours.	redundant functionality, but did so more than 150 calendar days but less than or equal to 180 calendar days since the previous test; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 6 hours and less than or equal to 8 hours.	redundant functionality, but did so more than 180 calendar days since the previous test; OR The Reliability Coordinator did not test its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality; OR The Reliability Coordinator tested its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, did not initiate action within 8 hours to restore the redundant functionality.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	N/A	N/A	N/A	The Reliability Coordinator failed to provide its System Operator with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities.
R5.	N/A	N/A	N/A	The Reliability Coordinator did not monitor Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.	N/A	N/A	N/A	The Reliability Coordinator did not have monitoring systems that provide information utilized by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant infrastructure.

D. Regional Variance

A. Regional Variance for the Western Electricity Coordinating Council Region

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) region.

Purpose
To develop a methodology that creates models for performing Operational Planning Analyses and Real-time Assessments.

Applicability
As used in this WECC Regional Variance, Reliability Coordinator is specific to those Reliability Coordinators providing Reliability Coordinator service(s) to entities operating within the Western Interconnection, regardless of where the Reliability Coordinator may be located.

Requirements and Measures

D.A.7. Each Reliability Coordinator shall, in coordination with other Reliability Coordinators, develop a common Interconnection-wide methodology to determine the modeling and monitoring of BES and non-BES Elements that are internal and external to its Reliability Coordinator Area, necessary for providing operational awareness of the impacts on Bulk Electric System Facilities within its Reliability Coordinator Area, including at a minimum: *([Violation Risk Factor: High] [Time Horizon: Operations Planning])*

- **D.A.7.1.** A method for development, maintenance, and periodic review of a Western Interconnection-wide reference model to serve as the baseline from which Reliability Coordinator's operational models are derived;
- **D.A.7.2.** The impacts of Inter-area oscillations;
- **D.A.7.3.** A method to determine Contingencies included in analyses and assessments;
- **D.A.7.4.** A method to determine Remedial Action Schemes included in analyses and assessments;
- **D.A.7.5.** A method to determine forecast data included in analyses and assessments; and
- **D.A.7.6.** A method for the validation and periodic review of the Reliability Coordinator's operational model for steady state and dynamic/oscillatory system response.

M.D.A.7. Each Reliability Coordinator will have evidence that it developed a common Western Interconnection-wide methodology, addressing modeling and

monitoring, in coordination with other Reliability Coordinators, that includes the features required in D.A.7.

D.A.8. Each Reliability Coordinator shall use the methodology developed in D.A.7. ([*Violation Risk Factor: High] [Time Horizon: Operations Planning*])

M.D.A.8. Each Reliability Coordinator will have evidence that it uses the methodology developed in D.A.7., as required in D.A.8. above.

Compliance

Evidence Retention:

- The Reliability Coordinator shall keep data or evidence for Requirements R5, R6, and the WECC Regional Variance, and Measures M5, M6, and the WECC Regional Variance for the current calendar year and one previous calendar year.

R #	Violation Severity Levels for the WECC Regional Variance			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
D.A.7.				The Reliability Coordinator did not develop the methodology as required in D.A.7.
D.A.8.				The Reliability Coordinator did not implement the methodology as required in D.A.8.

E. 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	November 1, 2006	Adopted by Board of Trustees	Revised
1	April 4, 2007	Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs) Corrected typographical errors in BOT approved version of VSLs	Revised to add missing measures and compliance elements
2	October 17, 2008	Adopted by NERC Board of Trustees	Deleted R2, M3 and associated compliance elements as conforming changes associated with approval of IRO-010-1. Revised as part of IROL Project
2	March 17, 2011	Order issued by FERC approving IRO-002-2 (approval effective 5/23/11)	FERC approval
2	February 24, 2014	Updated VSLs based on June 24, 2013 approval.	VSLs revised
3	July 25, 2011	Revised under Project 2006-06	Revised
3	August 4, 2011	Approved by Board of Trustees	Retired R1-R8 under Project 2006-06.
4	November 13, 2014	Approved by Board of Trustees	Revisions under Project 2014-03
4	November 19, 2015	FERC approved IRO-002-4. Docket No. RM15-16-000	FERC approval
5	February 9, 2017	Adopted by Board of Trustees	Revised

5	April 17, 2017	FERC letter Order approved IRO-002-5. Docket No. RD17-4-000	
6	May 9, 2019	Adopted by the NERC Board of Trustees	WECC Regional Variance
7	May 9, 2019	Adopted by the NERC Board of Trustees	Requirement R1 retired as part of Project 2018-03 Standards Efficiency Review Retirements.
7	September 17, 2020	FERC Order issued approving IRO-002-7. Docket No. RM19-16-000, RM19-17-000	
7	December 14,2020		FERC Approval
7	April 1, 2021	Effective Date	

Guidelines and Technical Basis

None.

Rationale

Rationale text from the development of IRO-002-4 in Project 2014-03 and IRO-002-5 in Project 2016-01 follows. Additional information can be found on the Project 2014-03 project page and the Project 2016-01 project page.

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 Requirements:
The data exchange elements of Requirements R1 and R2 from approved IRO-002-2 have been added back into proposed IRO-002-4 in order to ensure that there is no reliability gap. The Project 2014-03 SDT found no proposed requirements in the current project that covered the issue. Voice communication is covered in proposed COM-001-2 but data communications needs to remain in IRO-002-4 as it is not covered in proposed COM-001-2. Staffing of communications and facilities in corresponding requirements from IRO-002-2 is addressed in approved PER-004-2, Requirement R1 and has been deleted from this draft.

Rationale for R2:
Requirement R2 from IRO-002-3 has been deleted because approved EOP-008-1, Requirement R1, part 1.6.2 addresses redundancy and back-up concerns for outages of analysis tools. New Requirement R4 (R6 in IRO-002-5) has been added to address NOPR paragraphs 96 and 97: *"…As we explain above, the reliability coordinator's obligation to monitor SOLs is important to reliability because a SOL can evolve into an IROL during deteriorating system conditions, and for potential system conditions such as this, the reliability coordinator's monitoring of SOLs provides a necessary backup function to the transmission operator…."*

Rationale for Requirements R1 and R2: (*note*: R1 proposed for retirement in IRO-002-7 as part of Project 2018-03 Standard Efficiency Review Retirements)
The proposed changes address directives for redundancy and diverse routing of data exchange capabilities (FERC Order No. 817 Para 47).

Redundant and diversely routed data exchange capabilities consist of data exchange infrastructure components (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data) that will provide continued functionality despite failure or malfunction of an individual component within the Reliability Coordinator's (RC) primary

Control Center. Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. Requirement R2 does not require automatic or instantaneous fail-over of data exchange capabilities. Redundancy and diverse routing may be achieved in various ways depending on the arrangement of the infrastructure or hardware within the RC's primary Control Center.

The reliability objective of redundancy is to provide for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

Infrastructure that is not within the RC's primary Control Center is not addressed by the proposed requirement.

Rationale for Requirement R3:
The revised requirement addresses directives for testing of data exchange capabilities used in primary Control Centers (FERC Order No. 817 Para 51).

A test for redundant functionality demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data). An entity's testing practices should, over time, examine the various failure modes of its data exchange capabilities. When an actual event successfully exercises the redundant functionality, it can be considered a test for the purposes of the proposed requirement.

Rationale for R4 (R6 in IRO-002-5 and IRO-002-7):
The requirement was added back from approved IRO-002-2 as the Project 2014-03 SDT found no proposed requirements that covered the issues.

A. Introduction

1. **Title:** Reliability Coordinator Data Specification and Collection
2. **Number:** IRO-010-4
3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring the Reliability Coordinator has the data it needs to monitor and assess the operation of its Reliability Coordinator Area.
4. **Applicability**
   - **4.1.** Reliability Coordinator
   - **4.2.** Balancing Authority
   - **4.3.** Generator Owner
   - **4.4.** Generator Operator
   - **4.5.** Transmission Operator
   - **4.6.** Transmission Owner
   - **4.7.** Distribution Provider
5. **Effective Date*:** See BC Implementation Plan for Project 2019-06.

B. Requirements

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to: *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

- **1.1.** A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.
- **1.2.** Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.
- **1.3.** Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:
  - **1.3.1** Operating limitations based on:
    - **1.3.1.1.** capability and availability;
    - **1.3.1.2.** fuel supply and inventory concerns;
    - **1.3.1.3.** fuel switching capabilities; and
    - **1.3.1.4.** environmental constraints

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. A periodicity for providing data.

1.5. The deadline by which the respondent is to provide the indicated data.

M1. The Reliability Coordinator shall make available its dated, current, in force documented specification for data.

R2. The Reliability Coordinator shall distribute its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

M2. The Reliability Coordinator shall make available evidence that it has distributed its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. This evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R3. Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall satisfy the obligations of the documented specifications using: *(Violation Risk Factor: Medium) (Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations)*

3.1. A mutually agreeable format

3.2. A mutually agreeable process for resolving data conflicts

3.3. A mutually agreeable security protocol

M3. The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall make available evidence that it satisfied the obligations of the documented specification using the specified criteria. Such evidence could include but is not limited to electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
The British Columbia Utilities Commission.

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

The Reliability Coordinator shall retain its dated, current, in force documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.

The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.

Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

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#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include two or fewer of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
						monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
				Real-time Assessments.	Real-time Assessments.	Real-time Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow one of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow two of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow any of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

BC Implementation Plan for Project 2019-06.

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO-010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
4	TBD	Adopted by NERC Board of Trustees	Revisions under Project 2019-06 Cold Weather
3	October 30, 2020	FERC approved IRO-010-2. Docket No. RD20-4-000	
4	June 11, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06
4	August 24,2021	FERC approved IRO-010-4 Docket No. RD21-5-000	
4	August 24, 2021	April 1, 2023	Effective Date

A. Introduction

1. Title: Protection System Misoperation Identification and Correction

2. Number: PRC-004-6

3. Purpose: Identify and correct the causes of Misoperations of Protection Systems for Bulk Electric System (BES) Elements.

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 for BES Elements, with the following exclusions:

4.2.1.1 Non-protective functions that are embedded within a Protection System.

4.2.1.2 Protective functions intended to operate as a control function during switching.[1]

4.2.1.3 Special Protection Systems (SPS).

4.2.1.4 Remedial Action Schemes (RAS).

4.2.1.5 Protection Systems of individual dispersed power producing resources identified under Inclusion I4 of the BES definition where the Misoperations affected an aggregate nameplate rating of less than or equal to 75 MVA of BES Facilities.

4.2.2 Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.

4.2.3 Undervoltage load shedding (UVLS) that is intended to trip one or more BES Elements.

5. Effective Date*: See Implementation Plan.

[1] For additional information and examples, see the "Non-Protective Functions" and "Control Functions" sections in the Application Guidelines.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated under the circumstances in Parts 1.1 through 1.3 shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation: *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

1.1 The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and

1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and

1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation or was caused by manual intervention in response to its Protection System failure to operate.

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified the Misoperation of its Protection System component(s), if any, that meet the circumstances in Requirement R1, Parts 1.1, 1.2, and 1.3 within the allotted time period. Acceptable evidence for Requirement R1, including Parts 1.1, 1.2, and 1.3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, provide notification as described in Parts 2.1 and 2.2. *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

2.1 For a BES interrupting device operation by a Composite Protection System or by manual intervention in response to a Protection System failure to operate, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances:

2.1.1 The BES interrupting device owner shares the Composite Protection System ownership with any other owner; and

2.1.2 The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and

2.1.3 The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation.

2.2 For a BES interrupting device operation by a Protection System component intended to operate as backup protection for a condition on another entity's BES Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided.

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates notification to the other owner(s), within the allotted time period for either Requirement R2, Part 2.1, including subparts 2.1.1, 2.1.2, and 2.1.3 and Requirement R2, Part 2.2. Acceptable evidence for Requirement R2, including Parts 2.1 and 2.2 may include, but is not limited to the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, identify whether its Protection System component(s) caused a Misoperation. *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

M3. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified whether its Protection System component(s) caused a Misoperation within the allotted time period. Acceptable evidence for Requirement R3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, DME records, test results, or transmittals.

R4. Reserved.

M4. Reserved.

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation: [*Violation Risk Factor: High*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations; or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it developed a CAP and an evaluation of the CAP's applicability to other Protection Systems and locations, or a declaration in accordance with Requirement R5. Acceptable evidence for Requirement R5 may include, but is not limited to the following dated documentation (electronic or hardcopy format): CAP and evaluation, or declaration.

R6. Each Transmission Owner, Generator Owner, and Distribution Provider shall

implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed. *[Violation Risk Factor: High][Time Horizon: Operations Planning, Long-Term Planning]*

M6. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it implemented each CAP, including updating actions or timetables. Acceptable evidence for Requirement R6 may include, but is not limited to the following dated documentation (electronic or hardcopy format): records that document the implementation of each CAP and the completion of actions for each CAP including revision history of each CAP. Evidence may also include work management program records, work orders, and maintenance records.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority (CEA)

The British Columbia Utilities Commission.

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 Transmission Owner, Generator Owner, and Distribution Provider 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 Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, and R3, Measures M1, M2, and M3 for a minimum of 12 calendar months following the completion of each Requirement.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R5, Measure M5, including any supporting analysis per Requirements R1, R2, and R3, for a minimum of 12 calendar months following completion of each CAP, completion of each evaluation, and completion of each declaration.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R6, Measure M6 for a minimum of 12 calendar months following completion of each CAP.

If a Transmission Owner, Generator Owner, or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation

- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None**.**

Violation Severity Levels

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Operations Assessment, Operations Planning	High	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to identify whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	Operations Assessment, Operations Planning	High	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to notify one or more of the other owner(s) of the Protection System component(s) in accordance with Requirement R2.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	Operations Assessment, Operations Planning	High	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was less than or equal to 30 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 30 calendar days and less than or equal to 45 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 45 calendar days and less than or equal to 60 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 60 calendar days late. OR The responsible entity failed to identify whether or not a Misoperation of its Protection System component(s) occurred in accordance with Requirement R3.
R4. Reserved.						

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.	Operations Planning, Long-Term Planning	High	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop a CAP or explain in a declaration in accordance with Requirement R5. OR

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop an evaluation in accordance with Requirement R5.
R6.	Operations Planning, Long-Term Planning	High	The responsible entity implemented, but failed to update a CAP, when actions or timetables changed, in accordance with Requirement R6.	N/A	N/A	The responsible entity failed to implement a CAP in accordance with Requirement R6.

D. Regional Variances

None.

E. Associated Documents

NERC System Protection and Controls Subcommittee of the NERC Planning Committee, Assessment of Standards: PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems, PRC-004-1 – Analysis and Mitigation of Transmission and Generation Protection Misoperations, PRC-016-1 – Special Protection System Misoperations, May 22, 2009.[2]

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/06
1a	February 17, 2011	Adopted by NERC Board of Trustees	Project 2009-17 interpretation adding Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers
1a	September 26, 2011	Appended FERC-approved interpretation of R1 and R3 to version 1	FERC's Order approving the interpretation of R1 and R3 is effective as of September 26, 2011
2	August 5, 2010	Adopted by NERC Board of Trustees	Project 2010-12 modifications to address Order No. 693 Directives contained in paragraph 1469

[2] (http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/PRC-003-004-016%20Report.pdf).

Version	Date	Action	Change Tracking
2a	September 26, 2011	Appended FERC-approved interpretation of R1 and R3 to version 2	FERC's Order approving the interpretation of R1 and R3 is effective as of September 26, 2011
2.1a	February 9, 2012	Adopted by NERC Board of Trustees	Errata change under Project 2010-07 to add "…and generator interconnection Facility…"
3	August 14, 2014	Adopted by NERC Board of Trustees	Revision under Project 2010-05.1
4	November 13, 2014	Adopted by NERC Board of Trustees	Applicability revision under Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources
5	May 7, 2015	Adopted by NERC Board of Trustees	Revision under Project 2008-02.2
5(i)	June 22, 2015	Adopted by NERC Board of Trustees	Revision to VRF designations from "Medium" to "High" for Requirements R1 through R6, in compliance with the Federal Energy Regulatory Commission's directive in N. Am. Elec. Reliability Corp., 151 FERC ¶ 61,129 (2015)
6	May 9, 2019	Adopted by the NERC Board of Trustees	R4 retired under Project 2018-03 Standards Efficiency Review Retirements.
6	September 17, 2020	FERC Order issued approving PRC-004-6. Docket No. RM19-16-000, RM19-17-000	
6	December 14,2020		FERC Approval
6	April 1, 2021	Effective Date	

Guidelines and Technical Basis

Introduction

This standard addresses the reliability issues identified in the letter[3] from Gerry Cauley, NERC President and CEO, dated January 7, 2011.

> "Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure. …Relays can misoperate, either operate when not needed or fail to operate when needed, for a number of reasons. First, the device could experience an internal failure – but this is rare. Most commonly, relays fail to operate correctly due to incorrect settings, improper coordination (of timing and set points) with other devices, ineffective maintenance and testing, or failure of communications channels or power supplies. Preventable errors can be introduced by field personnel and their supervisors or more programmatically by the organization."

The standard also addresses the findings in the *2011 Risk Assessment of Reliability Performance*[4]; July 2011.

> "…a number of multiple outage events were initiated by protection system Misoperations. These events, which go beyond their design expectations and operating procedures, represent a tangible threat to reliability. A deeper review of the root causes of dependent and common mode events, which include three or more automatic outages, is a high priority for NERC and the industry."

The *State of Reliability 2014*[5] report continued to identify Protection System Misoperations as a significant contributor to automatic transmission outage severity. The report recommended completion of the development of PRC-004-3 as part of the solution to address Protection System Misoperations.

Definitions

The Misoperation definition is based on the IEEE/PSRC Working Group I3 "Transmission Protective Relay System Performance Measuring Methodology[6]." Misoperations of a Protection System include failure to operate, slowness in operating, or operating when not required either during a Fault or non-Fault condition.

For reference, a "Protection System" is defined in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary") as:

---

[3] (http://www.nerc.com/pa/Stand/Project%20201005%20Protection%20System%20Misoperations%20DL/20110209130708-Cauley%20letter.pdf).

[4] "2011 Risk Assessment of Reliability Performance." NERC. (http://www.nerc.com/files/2011_RARPR_FINAL.pdf. July 2011). Pg. 3.

[5] "State of Reliability 2014." NERC. (http://www.nerc.com/pa/Stand/Pages/RelaibilityCoordinationProject20066.aspx). May 2014. Pg. 18 of 106.

[6] "Transmission Protective Relay System Performance Measuring Methodology." Working Group I3 of Power System Relaying Committee of IEEE Power Engineering Society. 1999.

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

A BES interrupting device is a BES Element, typically a circuit breaker or circuit switcher that has the capability to interrupt fault current. Although BES interrupting device mechanisms are not part of a Protection System, the standard uses the operation of a BES interrupting device by a Protection System to initiate the review for Misoperation.

The following two definitions are being proposed for inclusion in the NERC Glossary:

> **Composite Protection System –** *The total complement of Protection System(s) that function collectively to protect an Element. Backup protection provided by a different Element's Protection System(s) is excluded.*

The Composite Protection System definition is based on the principle that an Element's multiple layers of protection are intended to function collectively. This definition has been introduced in this standard and incorporated into the proposed definition of Misoperation to clarify that the overall performance of an Element's total complement of protection should be considered while evaluating an operation.

Composite Protection System – Line Example
The Composite Protection System of the Alpha-Beta line (Circuit #123) is comprised of current differential, permissive overreaching transfer trip (POTT), step distance (classic zone 1, zone 2, and zone 3), instantaneous-overcurrent, time-overcurrent, out-of-step, and overvoltage protection. The protection is housed at the Alpha and Beta substations, and includes the associated relays, communications systems, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Transformer Example
The Composite Protection System of the Alpha transformer (#2) is comprised of internal differential, overall differential, instantaneous-overcurrent, and time-overcurrent protection. The protection is housed at the Alpha substation, and includes the associated relays, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Generator Example
The Composite Protection System of the Beta generator (#3) is comprised of generator differential, overall differential, overcurrent, stator ground, reverse power, volts per hertz, loss-of-field, and undervoltage protection. The protection is housed at the Beta generating plant and at the Beta substation, and includes the associated relays, voltage and current sensing

devices, DC supplies, and control circuitry.

Composite Protection System – Breaker Failure Example

Breaker failure protection provides backup protection for the breaker, and therefore is part of the breaker's Composite Protection System. Considering breaker failure protection to be part of another Element's Composite Protection System could lead to an incorrect conclusion that a breaker failure operation automatically satisfies the "Slow Trip" criteria of the Misoperation definition.

- An example of a correct operation of the breaker's Composite Protection System is when the breaker failure relaying tripped because the line relaying operated, but the breaker failed to clear the Fault. The breaker failure relaying operated because of a failed trip coil. The failed trip coil caused a Misoperation of the line's Composite Protection System.
- An example of a correct operation of the breaker's Composite Protection System is when the breaker failure relaying tripped because the line relaying operated, but the breaker failed to clear the Fault. Only the breaker failure relaying operated because of a failed breaker mechanism. This was not a Misoperation because the breaker mechanism is not part of the breaker's Composite Protection System.
- An example of an "Unnecessary Trip – During Fault" is when the breaker failure relaying tripped at the same time as the line relaying during a Fault. The Misoperation was due to the breaker failure timer being set to zero.

Misoperation – *The failure a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation:*

1. **Failure to Trip – During Fault** – *A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*
2. ***Failure to Trip – Other Than Fault*** – *A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*
3. ***Slow Trip – During Fault*** – *A Composite Protection System operation that is slower than required for a Fault condition if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.*
4. ***Slow Trip – Other Than Fault*** – *A Composite Protection System operation that is slower than required for a non-Fault condition, such as a power swing, undervoltage, overexcitation, or loss of excitation, if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.*
5. ***Unnecessary Trip – During Fault*** – *An unnecessary Composite Protection System operation for a Fault condition on another Element.*
6. ***Unnecessary Trip – Other Than Fault*** – *An unnecessary Composite Protection System*

operation for a non-Fault condition. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.

The Misoperation definition is based on the principle that an Element's total complement of protection is intended to operate dependably and securely.

- Failure to automatically reclose after a Fault condition is not included as a Misoperation because reclosing equipment is not included within the definition of Protection System.
- A breaker failure operation does not, in itself, constitute a Misoperation.
- A remote backup operation resulting from a "Failure to Trip" or a "Slow Trip" does not, in itself, constitute a Misoperation.

This proposed definition of Misoperation provides additional clarity over the current version. A Misoperation is the failure of a Composite Protection System to operate as intended for protection purposes. The definition includes six categories which provide further differentiation of what constitutes a Misoperation. These categories are discussed in greater detail in the following sections.

Failure to Trip – During Fault

This category of Misoperation typically results in the Fault condition being cleared by remote backup Protection System operation.

Example 1a: A failure of a transformer's Composite Protection System to operate for a transformer Fault is a Misoperation.

Example 1b: A failure of a "primary" transformer relay (or any other component) to operate for a transformer Fault is not a "Failure to Trip – During Fault" Misoperation as long as another component of the transformer's Composite Protection System operated.

Example 1c: A lack of target information does not by itself constitute a Misoperation. When a high-speed pilot system does not target because a high-speed zone element trips first, it would not in and of itself be a Misoperation.

Example 1d: A failure of an overall differential relay to operate is not a "Failure to Trip – During Fault" Misoperation as long as another component such as a generator differential relay operated.

Example 1e: The Composite Protection System for a bus does not operate during a bus Fault which results in the operation of all local transformer Protection Systems connected to that bus and all remote line Protection Systems connected to that bus isolating the faulted bus from the grid. The operation of the local transformer Protection Systems and the operation of all remote line Protection Systems correctly provided backup protection. There is one "Failure to Trip – During Fault" Misoperation of the bus Composite Protection System.

In analyzing the Protection System for Misoperation, the entity must also consider whether the "Slow Trip – During Fault" category applies to the operation.

Failure to Trip – Other Than Fault

This category of Misoperation may have resulted in operator intervention. The "Failure to Trip – Other Than Fault" conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

Example 2a: A failure of a generator's Composite Protection System to operate for an unintentional loss of field condition is a Misoperation.

Example 2b: A failure of an overexcitation relay (or any other component) is not a "Failure to Trip – Other Than Fault" Misoperation as long as the generator's Composite Protection System operated as intended isolating the generator from the BES.

In analyzing the Protection System for Misoperation, the entity must also consider whether the "Slow Trip – Other Than Fault" category applies to the operation.

Slow Trip – During Fault

This category of Misoperation typically results in remote backup Protection System operation before the Fault is cleared.

Example 3a: A Composite Protection System that is slower than required for a Fault condition is a Misoperation if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System. The current differential element of a multiple function relay failed to operate for a line Fault. The same relay's time-overcurrent element operated after a time delay. However, an adjacent line also operated from a time-overcurrent element. The faulted line's time-overcurrent element was found to be set to trip too slowly.

Example 3b: A failure of a breaker's Composite Protection System to operate as quickly as intended to meet the expected critical Fault clearing time for a line Fault in conjunction with a breaker failure (i.e., stuck breaker) is a Misoperation if it resulted in an unintended operation of at least one other Element's Composite Protection System. If a generating unit's Composite Protection System operates due to instability caused by the slow trip of the breaker's Composite Protection System, it is not an "Unnecessary Trip – During Fault" Misoperation of the generating unit's Composite Protection System. This event would be a "Slow Trip – During Fault" Misoperation of the breaker's Composite Protection System.

Example 3c: A line connected to a generation interconnection station is protected with two independent high-speed pilot systems. The Composite Protection System for this line also includes step distance and time-overcurrent schemes in addition to the two pilot systems. During a Fault on this line, the two pilot systems fail to operate and the time-overcurrent scheme operates clearing the Fault with no generating units or other Elements tripping (i.e., no over-trips). This event is not a Misoperation.

The phrase “slower than required” means the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System. It would be impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and system stability by the owner(s) reviewing each Protection System operation.

The phrase “resulted in the operation of any other Composite Protection System” refers to the need to ensure that relaying operates in the proper or planned sequence (i.e., the primary relaying for a faulted Element operates before the remote backup relaying for the faulted Element).

In analyzing the Protection System for Misoperation, the entity must also consider the “Unnecessary Trip – During Fault” category to determine if an “unnecessary trip” applies to the Protection System operation of an Element other than the faulted Element.

If a coordination error was at the local terminal (i.e., set too slow), then it was a "Slow Trip," category of Misoperation at the local terminal.

Slow Trip – Other Than Fault

The phrase “slower than required” means the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System. It would be impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and system stability by the owner(s) reviewing each Protection System operation.

> **Example 4:** A phase to phase fault occurred on the terminals of a generator. The generator's Composite Protection System and a transmission line's Composite Protection System both operated in response to the fault. It was found during subsequent investigation that the generator protection contained an inappropriate time delay. This caused the transmission line's correctly set overreaching zone of protection to operate. This was a Misoperation of the generator’s Composite Protection System, but not of the transmission line’s Composite Protection System.

The “Slow Trip – Other Than Fault” conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

Unnecessary Trip – During Fault

An operation of a properly coordinated remote Protection System is not in and of itself a Misoperation if the Fault has persisted for a sufficient time to allow the correct operation of the

Composite Protection System of the faulted Element to clear the Fault. A BES interrupting device failure, a “failure to trip” Misoperation, or a “slow trip” Misoperation may result in a proper remote Protection System operation.

Example 5: An operation of a transformer's Composite Protection System which trips (i.e., over-trips) for a properly cleared line Fault is a Misoperation. The Fault is cleared properly by the faulted equipment's Composite Protection System (i.e., line relaying) without the need for an external Protection System operation resulting in an unnecessary trip of the transformer protection; therefore, the transformer Protection System operation is a Misoperation.

Example 5b: An operation of a line's Composite Protection System which trips (i.e., over-trips) for a properly cleared Fault on a different line is a Misoperation. The Fault is cleared properly by the faulted line's Composite Protection System (i.e., line relaying); however, elsewhere in the system, a carrier blocking signal is not transmitted (e.g., carrier ON/OFF switch found in OFF position) resulting in the operation of a remote Protection System, single-end trip of a non-faulted line. The operation of the Protection System for the non-faulted line is an unnecessary trip during a Fault. Therefore, the non-faulted line Protection System operation is an “Unnecessary Trip – During Fault” Misoperation.

Example 5c: If a coordination error was at the remote terminal (i.e., set too fast), then it was an "Unnecessary Trip – During Fault" category of Misoperation at the remote terminal.

Unnecessary Trip – Other Than Fault

Unnecessary trips for non-Fault conditions include but are not limited to: power swings, overexcitation, loss of excitation, frequency excursions, and normal operations.

Example 6a: An operation of a line's Composite Protection System due to a relay failure during normal operation is a Misoperation.

Example 6b: Tripping a generator by the operation of the loss of field protection during an off-nominal frequency condition while the field is intact is a Misoperation assuming the Composite Protection System was not intended to operate under this condition.

Example 6c: An impedance line relay trip for a power swing that entered the relay’s characteristic is a Misoperation if the power swing was stable and the relay operated because power swing blocking was enabled and should have prevented the trip, but did not.

Example 6d: Tripping a generator operating at normal load by the operation of a reverse power protection relay due to a relay failure is a Misoperation.

Additionally, an operation that occurs during a non-Fault condition but was initiated directly by on-site (i.e., real-time) maintenance, testing, inspection, construction, or commissioning is not a Misoperation.

Example 6e: A BES interrupting device operation that occurs at the remote end of a line

during a non-Fault condition because a direct transfer trip was initiated by system maintenance and testing activities at the local end of the line is not a Misoperation because of the maintenance exclusion in category 6 of the definition of "Misoperation."

The "on-site" activities at one location that initiates a trip to another location are included in this exemption. This includes operation of a Protection System when energizing equipment to facilitate measurements, such as verification of current circuits as a part of performing commissioning; however, once the maintenance, testing, inspection, construction, or commissioning activity associated with the Protection System is complete, the "on-site" Misoperation exclusion no longer applies, regardless of the presence of on-site personnel.

Special Cases

Protection System operations for these cases would not be a Misoperation.

Example 7a: A generator Protection System operation prior to closing the unit breaker(s) is not a Misoperation provided no in-service Elements are tripped.

This type of operation is not a Misoperation because the generating unit is not synchronized and is isolated from the BES. Protection System operations that occur when the protected Element is out of service and that do not trip any in-service Elements are not Misoperations. In some cases where zones of protection overlap, the owner(s) of Elements may decide to allow a Protection System to operate faster in order to gain better overall Protection System performance for an Element.

Example 7b: The high-side of a transformer connected to a line may be within the zone of protection of the supplying line's relaying. In this case, the line relaying is planned to protect the area of the high-side of the transformer and into its primary winding. In order to provide faster protection for the line, the line relaying may be designed and set to operate without direct coordination (or coordination is waived) with local protection for Faults on the high-side of the connected transformer. Therefore, the operation of the line relaying for a high-side transformer Fault operated as intended and would not be a Misoperation.

Below are examples of conditions that would be a Misoperation.

Example7c: A 230 kV shunt capacitor bank was released for operational service. The capacitor bank trips due to a settings error in the capacitor bank differential relay upon energization.

Example 7d: A 230/115 kV BES transformer bank trips out when being re-energized due to an incorrect operation of the transformer differential relay for inrush after being released for operational service. Only the high-side breaker opens since the low-side breaker had not yet been closed.

Non-Protective Functions

BES interrupting device operations which are initiated by non-protective functions, such as those associated with generator controls, excitation controls, or turbine/boiler controls, static

voltampere-reactive compensators (SVC), flexible ac transmission systems (FACTS), high-voltage dc (HVdc) transmission systems, circuit breaker mechanisms, or other facility control systems are not operations of a Protection System. The standard is not applicable to non-protective functions such as automation (e.g., data collection) or control functions that are embedded within a Protection System.

Control Functions

The entity must make a determination as to whether the standard is applicable to each operation of its Protection System in accordance with the provided exclusions in the standard's Applicability, see Section 4.2.1. The subject matter experts (SME) developing this standard recognize that entities use Protection Systems as part of a routine practice to control BES Elements. This standard is not applicable to operation of protective functions within a Protection System when intended for controlling a BES Element as a part of an entity's process or planned switching sequence. The following are examples of conditions to which this standard is not applicable:

> **Example 8a:** The reverse power protective function that operates to remove a generating unit from service using the entity's normal or routine process.
>
> **Example 8b:** The reverse power relay enables a permissive trip and the generator operator trips the unit.

The standard is not applicable to operation of the protective relay because its operation is intended as a control function as part of a controlled shutdown sequence for the generator. However, the standard remains applicable to operation of the reverse power relay when it operates for conditions not associated with the controlled shutdown sequence, such as a motoring condition caused by a trip of the prime mover.

The following is another example of a condition to which this standard is not applicable:

> **Example 8c:** Operation of a capacitor bank interrupting device for voltage control using functions embedded within a microprocessor based relay that is part of a Protection System.

The above are examples only, and do not constitute an all-inclusive list to which the standard is not applicable.

Extenuating Circumstances

In the event of a natural disaster or other extenuating circumstances, the December 20, 2012 Sanction Guidelines of the North American Electric Reliability Corporation, Section 2.8, Extenuating Circumstances, reads: "In unique extenuating circumstances causing or contributing to the violation, such as significant natural disasters, NERC or the Regional Entity may significantly reduce or eliminate Penalties." The Regional Entities to whom NERC has delegated authority will consider extenuating circumstances when considering any sanctions in relation to the timelines outlined in this standard.

The volume of Protection System operations tend to be sporadic. If a high rate of Protection System operations is not sustained, utilities will have an opportunity to catch up within the 120 day period.

Requirement Time Periods

The time periods within all the Requirements are distinct and separate. The applicable entity in Requirement R1 has 120 calendar days to identify whether a BES interrupting device operation is a Misoperation. Once the applicable entity has identified a Misoperation, it has completed its performance under Requirement R1. Identified Misoperations with an identified cause become subject to Requirement R5 and any subsequent Requirements as necessary.

In Requirement R2, the applicable entity has 120 calendar days, based on the date of the BES interrupting device operation, to provide notification to the other Protection System owners that meet the circumstances in Parts 2.1 and 2.2. For the case of an applicable entity that was notified (R3), it has the later of 120 calendar days from the date of the BES interrupting device operation or 60 calendar days of notification to identify whether its Protection System components caused a Misoperation.

Once a Misoperation is identified in either Requirement R1 or R3, and the applicable entity did not identify the cause(s) of the Misoperation, the time period for performing at least one investigative action every two full calendar quarters begins.

The time period in Requirement R5 begins when the Misoperation cause is first identified. The applicable entity is allotted 60 calendar days to perform one of the two activities listed in Requirement R5 (e.g., CAP or declaration) to complete its performance under Requirement R5.

Requirement R6 time period is determined by the actions and the associated timetable to complete those actions identified in the CAP. The time periods contained in the CAP may change from time to time and the applicable entity is required to update the timetable when it changes.

Time periods provided in the Requirements are intended to provide a reasonable amount of time to perform each Requirement. Performing activities in the least amount of time facilitates prompt identification of Misoperations, notification to other Protection System owners, identification of the cause(s), correction of the cause(s), and that important information is retained that may be lost due to time.

Requirement R1

This Requirement initiates a review of each BES interrupting device operation to identify whether or not a Misoperation may have occurred. Since the BES interrupting device owner typically monitors and tracks device operations, the owner is the logical starting point for identifying Misoperations of Protection Systems for BES Elements. A review is required when (1) a BES interrupting device operates that is caused by a Protection System or by manual intervention in response to a Protection System failure to operate, (2) regardless of whether the owner owns all or part of the Protection System component(s), and (3) the owner identified its Protection System component(s) as causing the BES interrupting device operation or was

caused by manual intervention in response to its Protection System failure to operate.

Since most Misoperations result in the operation of one or more BES interrupting devices, these operations initiate a review to identify any Misoperation. If an Element is manually isolated in response to a failure to operate, the manual isolation of the Element triggers a review for Misoperation.

> **Example R1a:** The failure of a loss of field relay on a generating unit where an operator takes action to isolate the unit.

Manual intervention may indicate a Misoperation has occurred, thus requiring the initiation of an investigation by the BES interrupting device owner.

For the case where a BES interrupting device did not operate and remote clearing occurs due to the failure of a Composite Protection System to operate, the BES interrupting device owner would still review the operation under Requirement R1. However, if the BES interrupting device owner determines that its Protection System component operated as backup protection for a condition on another entity's BES Element, the owner would provide notification of the operation to the other Protection System owner(s) under Requirement R2, Part 2.2.

Protection Systems are made of many components. These components may be owned by different entities. For example, a Generator Owner may own a current transformer that sends information to a Transmission Owner's differential relay. All of these components and many more are part of a Protection System. It is expected that all of the owners will communicate with each other, sharing information freely, so that Protection System operations can be analyzed, Misoperations identified, and corrective actions taken.

Each entity is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation regardless of the level of ownership. A combination of available information from resources such as counters, relay targets, Supervisory Control and Data Acquisition (SCADA) systems, or DME would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. In many cases, it will not be necessary to leverage all available data to determine whether or not a Misoperation occurred. The standard also allows an entity to classify an operation as a Misoperation if entity is not sure. The entity may decide to identify the operation as a Misoperation to satisfy Requirement R1 and continue its investigation for a cause of the Misoperation . If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation. The entity is allotted 120 calendar days from the date of its BES interrupting device operation to identify whether its Protection System component(s) caused a Misoperation.

The Protection System operation may be documented in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System.

Repeated operations which occur during the same automatic reclosing sequence do not need a

separate identification under Requirement R1. Repeated Misoperations which occur during the same 24-hour period do not need a separate identification under Requirement R1. This is consistent with the NERC *Misoperations Report*[7] which states:

> "In order to avoid skewing the data with these repeated events, the NERC SPCS should clarify, in the next annual update of the misoperation template, that all misoperations due to the same equipment and cause within a 24 hour period be recorded as one misoperation."

The following is an example of a condition that is not a Misoperation.

> **Example R1b:** A high impedance Fault occurs within a transformer. The sudden pressure relaying detects and operates for the Fault, but the differential relaying did not operate due to the low Fault current levels. This is not a Misoperation because the Composite Protection System was not required to operate because the Fault was cleared by the sudden pressure relay.

Requirement R2

Requirement R2 ensures notification of those who have a role in identifying Misoperations, but were not accounted for within Requirement R1. In the case of multi-entity ownership, the entity that owns the BES interrupting device that operated is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation under Requirement R1; however, if the entity that owns a BES interrupting device determines that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation, it must notify the other Protection System owner(s) that share Misoperation identification responsibility when the criteria in Requirement R2 is met.

This Requirement does not preclude the Protection System owners from initially communicating and working together to determine whether a Misoperation occurred and, if so, the cause. The BES interrupting device owner is only required to officially notify the other owners when it: (1) shares the Composite Protection System ownership with other entity(ies), (2) determines that a Misoperation occurred or cannot rule out a Misoperation, and (3) determines its Protection System component(s) did not cause a Misoperation or is unsure. Officially notifying the other owners without performing a preliminary review may unnecessarily burden the other owners with compliance obligations under Requirement R3, redirect valuable resources, and add little benefit to reliability. The BES interrupting device owner should officially notify other owners when appropriate within the established time period.

The following is an example of a notification to another Protection System owner:

> **Example R2a:** Circuit breakers A and B at the Charlie station tripped from directional

[7] "Misoperations Report." Reporting Multiple Occurrences. NERC Protection System Misoperations Task Force. (http://www.nerc.com/docs/pc/psmtf/PSMTF_Report.pdf). April 1, 2013. Pg. 37 of 40.

comparison blocking (DCB) relaying on 03/03/2014 at 15:43 UTC during an external Fault. As discussed last week, the fault records indicate that a problem with your equipment (failure to transmit) caused the operation.

Example R2b: A generator unit tripped out immediately upon synchronizing to the grid due to a Misoperation of its overcurrent protection. The Transmission Owner owns the 230 kV generator breaker that operated. The Transmission Owner, as the owner of the BES interrupting device after determining that its Protection System components did not cause the Misoperation, notified the Generator Owner of the operation. The Generator Owner investigated and determined that its Protection System components caused the Misoperation. In this example, the Generator Owner's Protection System components did cause the Misoperation. As the owner of the Protection System components that caused the Misoperation, the Generator Owner is responsible for creating and implementing the CAP.

A Composite Protection System owned by different functional entities within the same registered entity does not necessarily satisfy the notification criteria in Part 2.1.1 of Requirement R2. For example, if the same personnel within a registered entity perform the Misoperation identification for both the Generator Owner and Transmission Owner functions, then the Misoperation identification would be completely covered in Requirement R1, and therefore notification would not be required. However, if the Misoperation identification is handled by different groups, then notification would be required because the Misoperation identification would not necessarily be covered in Requirement R1.

Example R2c: Line A Composite Protection System (owned by entity 1) failed to operate for an internal Fault. As a result, the zone 3 portion of Line B's Composite Protection System (owned by entity 2) and zone 3 portion of Line C's Composite Protection System (owned by entity 3) operated to clear the Fault. Entity 2 and 3 notified entity 1 of the remote zone 3 operation.

For the case where a BES interrupting device operates to provide backup protection for a non-BES Element, the entity reviewing the operation is not required to notify the other owners of Protection Systems for non-BES Elements. No notification is required because this Reliability Standard is not applicable to Protection Systems for non-BES Elements.

Requirement R3

For Requirement R3 (i.e., notification received), the entity that also owns a portion of the Composite Protection System is expected to use judgment to identify whether the Protection System operation is a Misoperation. A combination of available information from resources such as counters, relay targets, SCADA, DME, and information from the other owner(s) would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. In many cases, it will not be necessary to leverage all available data to determine whether or not a Misoperation occurred. The standard also allows an entity to classify an operation as a Misoperation if an entity is not sure. The entity may decide to identify the operation as a Misoperation to satisfy Requirement R1 and continue its investigation for a

cause of the Misoperation. If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation.

The entity that is notified by the BES interrupting device owner is allotted the later of 60 calendar days from receipt of notification or 120 calendar days from the BES interrupting device operation date to determine if its portion of the Composite Protection System caused the Protection System operation. It is expected that in most cases of a jointly owned Protection System, the entity making notification would have been in communication with the other owner(s) early in the process. This means that the shorter 60 calendar days only comes into play if the notification occurs in the second half of the 120 calendar days allotted to the BES interrupting device owner in Requirement R1.

The Protection System review may be organized in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System. The BES interrupting device owner's notification received may be documented in a variety of ways such as an email or a facsimile.

Requirement R5

Resolving the causes of Protection System Misoperations benefits BES reliability by preventing recurrence. The Corrective Action Plan (CAP) is an established tool for resolving operational problems. The NERC Glossary defines a Corrective Action Plan as, *"A list of actions and an associated timetable for implementation to remedy a specific problem."* Since a CAP addresses specific problems, the determination of what went wrong needs to be completed before developing a CAP. When the Misoperation cause is identified in Requirement R1 or R3, Requirement R5 requires Protection System owner(s) to develop a CAP, or explain why corrective actions are beyond the entity's control or would not improve BES reliability. The entity must develop the CAP or make a declaration why additional actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken within 60 calendar days of first determining a cause.

The SMEs developing this standard recognize there may be multiple causes for a Misoperation. In these circumstances, the CAP would include a remedy for the identified causes. The CAP may be revised if additional causes are found; therefore, the entity has the option to create a single or multiple CAP(s) to correct multiple causes of a Misoperation. The 60 calendar day period for developing a CAP (or declaration) is established on the basis of industry experience which includes operational coordination timeframes, time to consider alternative solutions, coordination of resources, and development of a schedule.

The development of a CAP is intended to document the specific corrective actions needed to be taken to prevent Misoperation recurrence, the timetable for executing such actions, and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations. The evaluation of these other Protection Systems aims to reduce the risk and likelihood of similar Misoperations in other Protection Systems. The Protection System owner is responsible for determining the extent of its evaluation concerning other Protection Systems and locations. The evaluation may result in the owner including actions to address Protection

Systems at other locations or the reasoning for not taking any action. The CAP and an evaluation of other Protection Systems including other locations must be developed to complete Requirement R5.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined capacitor replacement was not necessary.

For completion of each CAP in Examples R5a through R5d, please see Examples R6a through R6d.

Example R5a: Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.

Applicability to other Protection Systems: This type of impedance relay has not been experiencing problems and is systematically being replaced with microprocessor relays as Protection Systems are modernized. Therefore, it was assessed that a program for wholesale preemptive replacement of capacitors in this type of impedance relay does not need to be established for the system.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

Example R5b: Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.

Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, a program should be established by 12/01/2014 for wholesale preemptive replacement of capacitors in this type of impedance relay.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

Example R5c: Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.

Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, the preemptive replacement of capacitors in this type of impedance relay should be pursued for the identified stations A through I by 04/30/2015.

A plan is being developed to replace the impedance relay capacitors at stations A, B, and C by 09/01/2014. A second plan is being developed to replace the impedance relay capacitors

at stations D, E, and F by 11/01/2014. The last plan will replace the impedance relay capacitors at stations G, H, and I by 02/01/2015.

The following is an example of a CAP for a relay Misoperation that was due to a version 2 firmware problem and the evaluation of the cause at similar locations which determined the firmware needs preemptive correction action.

Example R5d: Actions: Provide the manufacturer fault records. Install new firmware pending manufacturer results by 10/01/2014.

Applicability to other Protection Systems: Based on the evaluation of other locations and a risk assessment, the newer firmware version 3 should be installed at all installations that are identified to be version 2. Twelve relays were identified across the system. Proposed completion date is 12/31/2014.

The following are examples of a declaration made where corrective actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken.

Example R5e: The cause of the Misoperation was due to a non-registered entity communications provider problem.

Example R5f: The cause of the Misoperation was due to a transmission transformer tapped industrial customer who initiated a direct transfer trip to a registered entity's transmission breaker.

In situations where a Misoperation cause emanates from a non-registered outside entity, there may be limited influence an entity can exert on an outside entity and is considered outside of an entity's control.

The following are examples of declarations made why corrective actions would not improve BES reliability.

Example R5g: The investigation showed that the Misoperation occurred due to transients associated with energizing transformer ABC at Station Y. Studies show that de-sensitizing the relay to the recorded transients may cause the relay to fail to operate as intended during power system oscillations.

Example R5h: As a result of an operation that left a portion of the power system in an electrical island condition, circuit XYZ within that island tripped, resulting in loss of load within the island. Subsequent investigation showed an overfrequency condition persisted after the formation of that island and the XYZ line protective relay operated. Since this relay was operating outside of its designed frequency range and would not be subject to this condition when line XYZ is operated normally connected to the BES, no corrective action will be taken because BES reliability would not be improved.

Example R5i: During a major ice storm, four of six circuits were lost at Station A. Subsequent to the loss of these circuits, a skywire (i.e., shield wire) broke near station A on line AB (between Station A and B) resulting in a phase-phase Fault. The protection scheme utilized for both protection groups is a permissive overreaching transfer trip (POTT). The Line AB protection at Station B tripped timed for this event (i.e., Slow Trip – During Fault) even though this line had been identified as requiring high speed clearing. A weak infeed condition was created at Station A due to the loss of 4 transmission circuits resulting in the absence of a permissive signal on Line AB from Station A during this Fault. No corrective action will be taken for this Misoperation as even under N-1 conditions, there is normally enough infeed at Station A to send a proper permissive signal to station B. Any changes to the protection scheme to account for this would not improve BES reliability.

A declaration why corrective actions are beyond the entity's control or would not improve BES reliability should include the Misoperation cause and the justification for taking no corrective action. Furthermore, a declaration that no further corrective actions will be taken is expected to be used sparingly.

Requirement R6

To achieve the stated purpose of this standard, which is to identify and correct the causes of Misoperations of Protection Systems for BES Elements, the responsible entity is required to implement a CAP that addresses the specific problem (i.e., cause(s) of the Misoperation) through completion. Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until completed. Accomplishing this objective is intended to reduce the occurrence of future Misoperations of a similar nature, thereby improving reliability and minimizing risk to the BES.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip (See also, Example R5a).

Example R6a: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

CAP completed on 06/25/2014.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip that resulted in the correction and the establishment of a program for further replacements (See also, Example R5b).

Example R6b: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

A program for wholesale preemptive replacement of capacitors in this type of impedance

relay was established on 10/28/2014.

CAP completed on 10/28/2014.

The following is an example of a completed CAP of corrective actions with a timetable that required updating for a failed relay and preemptive actions for similar installations (See also, Example R5c).

Example R6c: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

The impedance relay capacitor replacement was completed at stations A, B, and C on 08/16/2014. The impedance relay capacitor replacement was completed at stations D, E, and F on 10/24/2014. The impedance relay capacitor replacement for stations G, H, and I were postponed due to resource rescheduling from a scheduled 02/01/15 completion to 04/01/2015 completion. Capacitor replacement was completed on 03/09/2015 at stations G, H, and I. All stations identified in the evaluation have been completed.

CAP completed on 03/09/2015.

The following is an example of a completed CAP for corrective actions with updated actions for a firmware problem and preemptive actions for similar installations. (See also, Example R5d).

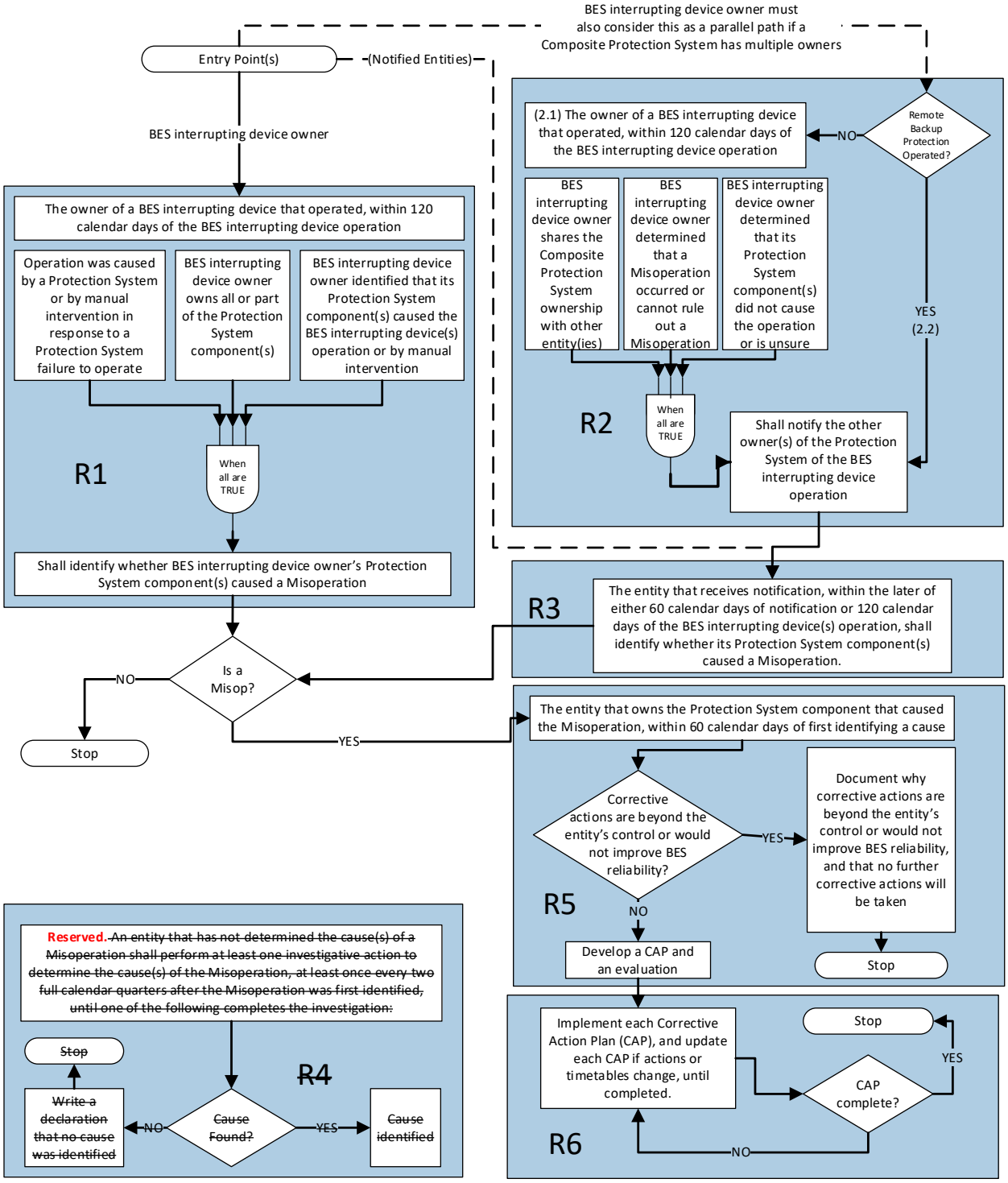
Example R6d: Actions: fault records were provided to the manufacturer on 06/04/2014. The manufacturer responded that the Misoperation was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. Version 3 firmware was installed on 08/12/2014.

Nine of the twelve relays were updated to version 3 firmware on 09/23/2014. The manufacturer provided a subsequent update which was determined to be beneficial for the remaining relays. The remaining three of twelve relays identified as having the version 2 firmware were updated to version 3.01 firmware on 11/10/2014.

CAP completed on 11/10/2014.

The CAP is complete when all of the actions identified within the CAP have been completed.

Process Flow Chart: Below is a graphical representation demonstrating the relationships between Requirements:



A. Introduction

1. **Title:** **Automatic Underfrequency Load Shedding**

2. **Number:** PRC-006-5

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

   4.2.3 UFLS-Only Distribution Providers

   4.3. Transmission Owners that own Elements identified in the UFLS program established by the Planning Coordinators.

5. **Effective Date:**

   See Implementation Plan

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-006-5 - 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-006-5 - 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-006-5 - 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-006-5 - 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-006-5 - 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-006-5 — 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-006-5 — 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-006-5 — 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

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 - 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 - 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 - 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 - 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 Interconnection and replaces, in their entirety, Requirements R1 through R5, and R11 through R15.

As used in the RV, Planning Coordinator is specific to those Planning Coordinators providing Planning Coordinator service(s) to entities within the Western Interconnection, regardless of where the Planning Coordinator is located.

D.B.1. Each Planning Coordinator shall participate in a joint regional review with the other Planning Coordinators 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 will have evidence such as reports, or other documentation of its criteria, developed as part of the joint regional review with other Planning Coordinators 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 Western Interconnection-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 Western Interconnection (planned islands) as a result of the operation of a relay scheme or Remedial Action Scheme.

M.D.B.2. Each Planning Coordinator will 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 Western Interconnection-wide coordinated UFLS program meeting 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 Western Interconnection, 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-006-5 - 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-006-5 - 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 will have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its adoption of a UFLS program, coordinated across the Western Interconnection, including the notification of the UFLS entities of implementation schedule meeting 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 Western Interconnection 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-006-5 - 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-006-5 - 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-006-5 - 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-006-5 — 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-006-5 — 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-006-5 — 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 will 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 demonstrating that it meets Requirement D.B.4 Parts D.B.4.1 through D.B.4.7.

D.B.5. through D.B.10. Reserved

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 will 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 all other Planning Coordinators in the Western Interconnection to consider the identified deficiencies within two years of event actuation. *[VRF: Medium][Time Horizon: Operations Assessment]*

M.D.B.12. Each Planning Coordinator will 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 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 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 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 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.B.2	N/A	N/A	The Planning Coordinator identified an island(s) from the	The Planning Coordinator identified an island(s) from the

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
			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	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 Western Interconnection 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 simulations of underfrequency conditions	The Planning Coordinator adopted a UFLS program, coordinated across the Western Interconnection 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 Western Interconnection 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 simulations of underfrequency conditions OR The Planning Coordinator failed to adopt a UFLS program,

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				coordinated across the Western Interconnection , 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 across the Western Interconnection 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 D.B.4, Parts D.B.4.1 through D.B.4.7.	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators across the Western Interconnection 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 Requirement D.B.4, Parts D.B.4.1 through D.B.4.7.	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators across the Western Interconnection 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 Requirement D.B.4, Parts D.B.4.1 through D.B.4.7.	The Planning Coordinator participated in and documented a coordinated UFLS assessment with the other Planning Coordinators across the Western Interconnection 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 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 across the Western

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Interconnection 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 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.	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 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.	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 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	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 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

D #	Lower VSL	Moderate VSL	High VSL	Severe VSL
			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.	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 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 #	Lower VSL	Moderate VSL	High VSL	Severe VSL
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 across the Western Interconnection 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 across the Western Interconnection 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 across the Western Interconnection 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 and document a coordinated UFLS design assessment of the coordinated UFLS program with the other Planning Coordinators across the Western Interconnection to consider the identified deficiencies

E. Associated Documents

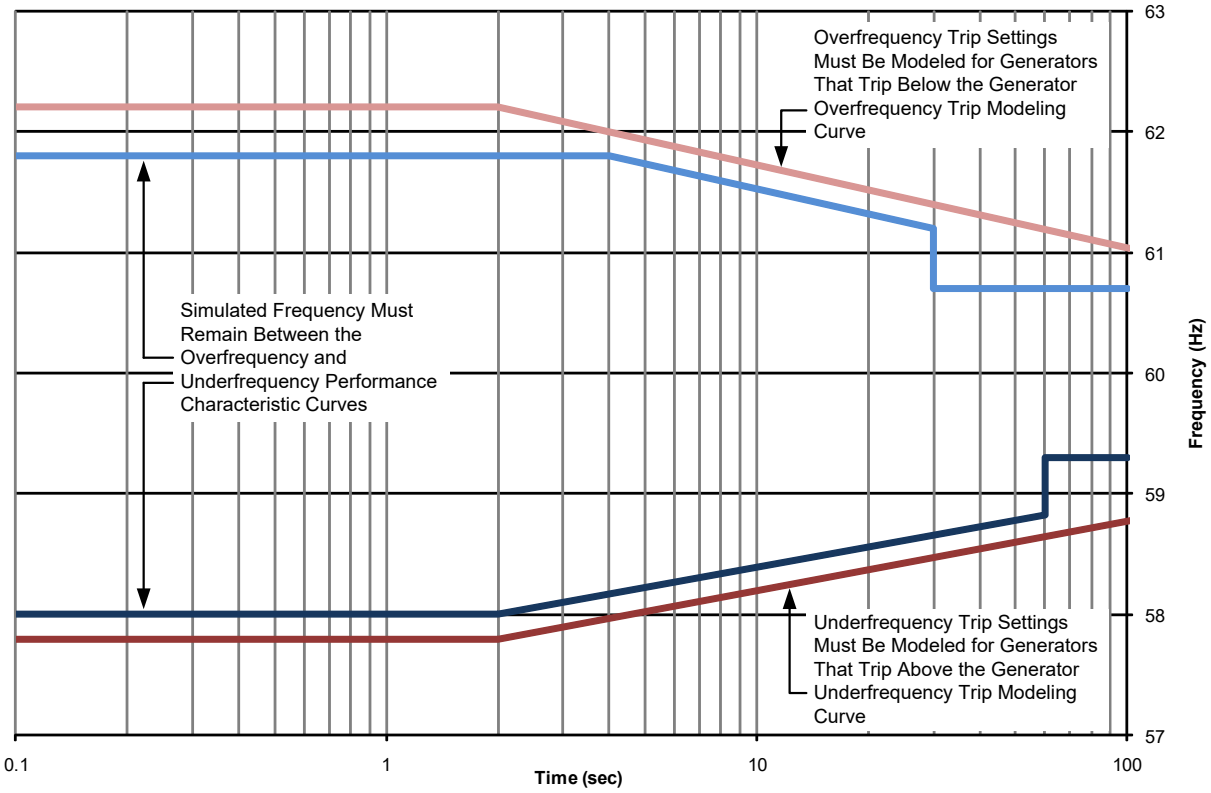
Version History

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.
2	March 4, 2015	FERC Order issued approving PRC-006-2. Docket No. RD15-2-000	
3	August 10, 2017	Adopted by the NERC Board of Trustees	Revisions to the Regional Variance for the Quebec Interconnection.
3	September 5, 2017	FERC Order issued approving PRC-006-3.	

4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
5	August 20, 2020	Adopted by NERC Board of Trustees	In Version 5: 1) Requirements R14 and R15 were added to the list of Requirements not applicable to the Western Interconnection (WI), 2) use of "Planning Coordinator" (PC) was made specific to PCs providing services within the WI, regardless of where the PC is located, 3) non-substantive changes were made conforming the document and styles to the newest NERC conventions and templates, and 4) references to Version 3 were updated to Version 5.
5	December 23,2020	FERC Oder approving PRC-006-5 Docket No. RD21-1-000	
5	April 1, 2021	Effective Date	

PRC-006-5 – 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



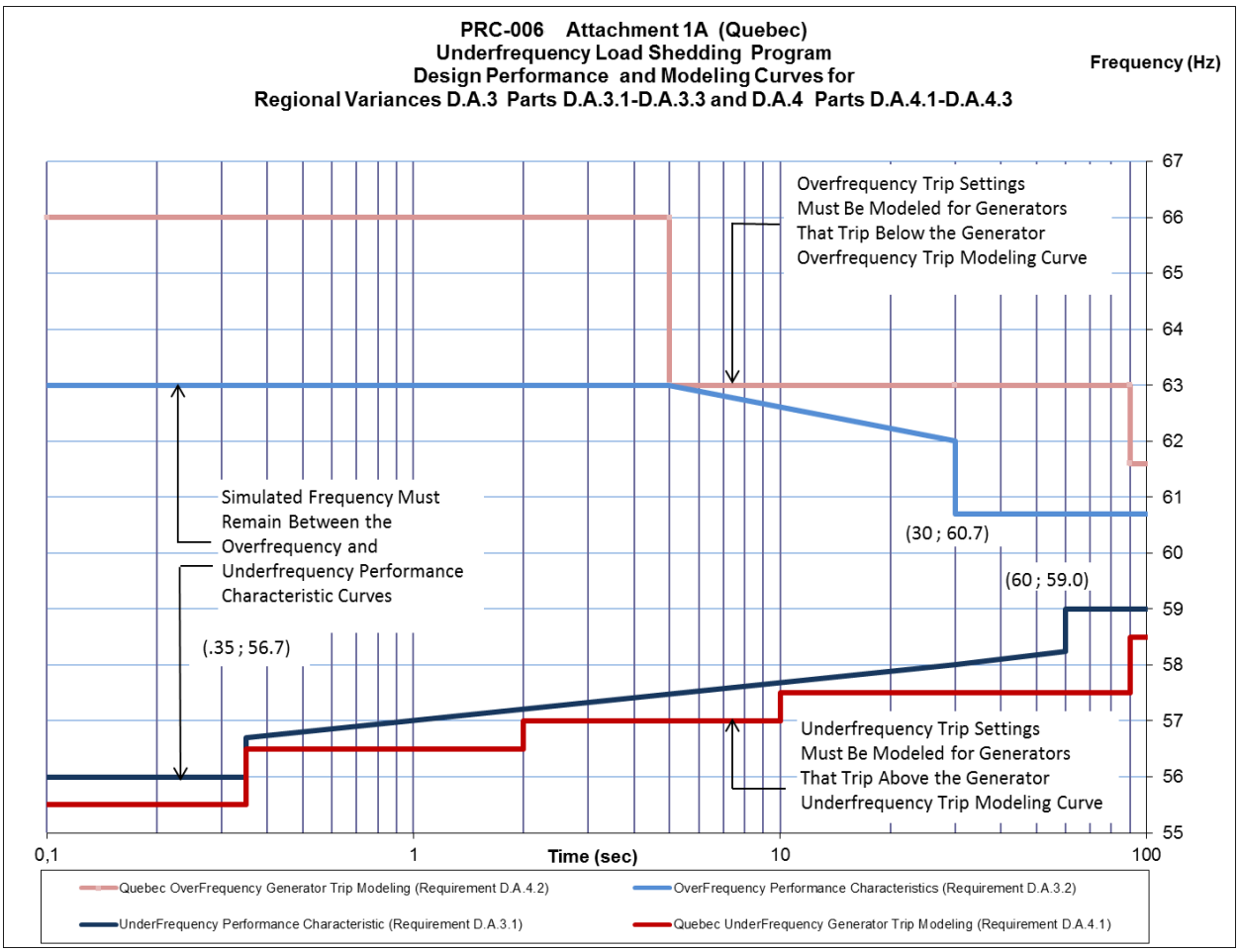
- Generator Overfrequency Trip Modeling (Requirement R4 Parts 4.4-4.6)
- Overfrequency Performance Characteristic (Requirement R3 Part 3.2)
- Underfrequency Performance Characteristic (Requirement R3 Part 3.1)
- Generator Underfrequency Trip Modeling (Requirement R4 Parts 4.1-4.3)

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 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.

A. Introduction

1. **Title:** Transmission Operations

2. **Number:** TOP-001-5

3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Interconnection by ensuring prompt action to prevent or mitigate such occurrences.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

   4.1.2. Transmission Operator

   4.1.3. Generator Operator

   4.1.4. Distribution Provider

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

B. Requirements and Measures

R1. Each Transmission Operator shall act to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions. *[Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]*

M1. Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.

R2. Each Balancing Authority shall act to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions. *[Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]*

M2. Each Balancing Authority shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions.

R3. Each Balancing Authority, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Transmission Operator(s), unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M3. Each Balancing Authority, Generator Operator, and Distribution Provider shall make available upon request, evidence that it complied with each Operating Instruction issued by the Transmission Operator(s) unless such action could not be physically implemented or it would have violated safety, equipment, regulatory, or statutory requirements. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. In such cases, the Balancing Authority, Generator Operator, and Distribution Provider shall have and provide copies of the safety, equipment, regulatory, or statutory requirements as evidence for not complying with the Transmission Operator's Operating Instruction. If such a situation has not occurred, the Balancing Authority, Generator Operator, or Distribution Provider may provide an attestation.

R4. Each Balancing Authority, Generator Operator, and Distribution Provider shall inform its Transmission Operator of its inability to comply with an Operating Instruction issued by its Transmission Operator. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M4. Each Balancing Authority, Generator Operator, and Distribution Provider shall make available upon request, evidence which may include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence in electronic or hard copy format, that it informed its Transmission Operator of its inability to comply with its Operating Instruction issued. If such a situation has not occurred, the Balancing Authority, Generator Operator, or Distribution Provider may provide an attestation.

R5. Each Transmission Operator, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Balancing Authority, unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M5. Each Transmission Operator, Generator Operator, and Distribution Provider shall make available upon request, evidence that it complied with each Operating Instruction issued by its Balancing Authority unless such action could not be physically implemented or it would have violated safety, equipment, regulatory, or statutory requirements. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. In such cases, the Transmission Operator, Generator Operator, and Distribution Provider shall have and provide copies of the safety, equipment, regulatory, or statutory requirements as evidence for not complying with the Balancing Authority's Operating Instruction. If such a situation has not occurred, the Transmission Operator, Generator Operator, or Distribution Provider may provide an attestation.

R6. Each Transmission Operator, Generator Operator, and Distribution Provider shall inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]*

M6. Each Transmission Operator, Generator Operator, and Distribution Provider shall make available upon request, evidence which may include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence in electronic or hard copy format, that it informed its Balancing Authority of its inability to comply with its Operating Instruction. If such a situation has not occurred, the Transmission Operator, Generator Operator, or Distribution Provider may provide an attestation.

R7. Each Transmission Operator shall assist other Transmission Operators within its Reliability Coordinator Area, if requested and able, provided that the requesting Transmission Operator has implemented its comparable Emergency procedures, unless such assistance cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M7. Each Transmission Operator shall make available upon request, evidence that comparable requested assistance, if able, was provided to other Transmission Operators within its Reliability Coordinator Area unless such assistance could not be physically implemented or would have violated safety, equipment, regulatory, or statutory requirements. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. If no request for assistance was received, the Transmission Operator may provide an attestation.

R8. Each Transmission Operator shall inform its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-Time Operations]*

M8. Each Transmission Operator shall make available upon request, evidence that it informed its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence. If no such situations have occurred, the Transmission Operator may provide an attestation.

R9. Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-Time Operations]*

M9. Each Balancing Authority and Transmission Operator shall make available upon request, evidence that it notified its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence. If such a situation has not occurred, the Balancing Authority or Transmission Operator may provide an attestation.

R10. Each Transmission Operator shall perform the following for determining System Operating Limit (SOL) exceedances within its Transmission Operator Area: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

10.1. Monitor Facilities within its Transmission Operator Area;

10.2. Monitor the status of Remedial Action Schemes within its Transmission Operator Area;

10.3. Monitor non-BES facilities within its Transmission Operator Area identified as necessary by the Transmission Operator;

10.4. Obtain and utilize status, voltages, and flow data for Facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator;

10.5. Obtain and utilize the status of Remedial Action Schemes outside its Transmission Operator Area identified as necessary by the Transmission Operator; and

10.6. Obtain and utilize status, voltages, and flow data for non-BES facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator.

M10. Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to Energy Management System description documents, computer printouts, Supervisory Control and Data Acquisition (SCADA) data collection, or other equivalent evidence that will be used to confirm that it monitored or obtained and utilized data as required to determine any System Operating Limit (SOL) exceedances within its Transmission Operator Area.

R11. Each Balancing Authority shall monitor its Balancing Authority Area, including the status of Remedial Action Schemes that impact generation or Load, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M11. Each Balancing Authority shall have, and provide upon request, evidence that could include but is not limited to Energy Management System description documents, computer printouts, SCADA data collection, or other equivalent evidence that will be used to confirm that it monitors its Balancing Authority Area, including the status of Remedial Action Schemes that impact generation or Load, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency.

R12. Each Transmission Operator shall not operate outside any identified Interconnection Reliability Operating Limit (IROL) for a continuous duration exceeding its associated IROL T_v. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M12. Each Transmission Operator shall make available evidence to show that for any occasion in which it operated outside any identified Interconnection Reliability Operating Limit (IROL), the continuous duration did not exceed its associated IROL T_v. Such evidence could include but is not limited to dated computer logs or reports in electronic or hard copy format specifying the date, time, duration, and details of the

excursion. If such a situation has not occurred, the Transmission Operator may provide an attestation that an event has not occurred.

R13. Each Transmission Operator shall ensure that a Real-time Assessment is performed at least once every 30 minutes. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M13. Each Transmission Operator shall have, and make available upon request, evidence to show it ensured that a Real-Time Assessment was performed at least once every 30 minutes. This evidence could include but is not limited to dated computer logs showing times the assessment was conducted, dated checklists, or other evidence.

R14. Each Transmission Operator shall initiate its Operating Plan to mitigate a SOL exceedance identified as part of its Real-time monitoring or Real-time Assessment. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

M14. Each Transmission Operator shall have evidence that it initiated its Operating Plan for mitigating SOL exceedances identified as part of its Real-time monitoring or Real-time Assessments. This evidence could include but is not limited to dated computer logs showing times the Operating Plan was initiated, dated checklists, or other evidence.

R15. Each Transmission Operator shall inform its Reliability Coordinator of actions taken to return the System to within limits when a SOL has been exceeded. *[Violation Risk Factor: Medium] [Time Horizon: Real-Time Operations]*

M15. Each Transmission Operator shall make available evidence that it informed its Reliability Coordinator of actions taken to return the System to within limits when a SOL was exceeded. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, or dated computer printouts. If such a situation has not occurred, the Transmission Operator may provide an attestation.

R16. Each Transmission Operator shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M16. Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to a documented procedure or equivalent evidence that will be used to confirm that the Transmission Operator has provided its System Operators with the authority to approve planned outages and maintenance of telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.

R17. Each Balancing Authority shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication

channels between affected entities. *[Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M17. Each Balancing Authority shall have, and provide upon request, evidence that could include but is not limited to a documented procedure or equivalent evidence that will be used to confirm that the Balancing Authority has provided its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.

R18. Each Transmission Operator shall operate to the most limiting parameter in instances where there is a difference in SOLs. [*Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

M18. Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to operator logs, voice recordings, electronic communications, or equivalent evidence that will be used to determine if it operated to the most limiting parameter in instances where there is a difference in SOLs.

R19. Reserved.

M19. Reserved.

R20. Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M20. Each Transmission Operator shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order to perform its Real-time monitoring and Real-time Assessments as specified in the requirement.

R21. Each Transmission Operator shall test its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Transmission Operator shall initiate action within two hours to restore redundant functionality. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M21. Each Transmission Operator shall have, and provide upon request, evidence that it tested its primary Control Center data exchange capabilities specified in Requirement R20 for the redundant functionality, or experienced an event that demonstrated the

redundant functionality; and, if the test was unsuccessful, initiated action within two hours to restore redundant functionality as specified in Requirement R21. Evidence could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, or electronic communications.

R22. Reserved.

M22. Reserved.

R23. Each Balancing Authority shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Balancing Authority's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Transmission Operator, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and analysis functions. *[Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]*

M23. Each Balancing Authority shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Balancing Authority's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Transmission Operator, and the entities it has identified it needs data from in order to perform its Real-time monitoring and analysis functions as specified in the requirement.

R24. Each Balancing Authority shall test its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Balancing Authority shall initiate action within two hours to restore redundant functionality. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M24. Each Balancing Authority shall have, and provide upon request, evidence that it tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, or experienced an event that demonstrated the redundant functionality; and, if the test was unsuccessful, initiated action within two hours to restore redundant functionality as specified in Requirement R24. Evidence could include, but is not limited to: dated and time-stamped test records, operator logs, voice recordings, or electronic communications.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The British Columbia Utilities Commission.

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 Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicable Requirement R1 through R11, and Measure M1 through M11, 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.
- Each Transmission Operator shall retain evidence for three calendar years of any occasion in which it has exceeded an identified IROL and its associated IROL T_v as specified in Requirement R12 and Measure M12.
- Each Transmission Operator shall keep data or evidence for Requirement R13 and Measure M13 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.
- Each Transmission Operator shall retain evidence and that it initiated its Operating Plan to mitigate a SOL exceedance as specified in Requirement R14 and Measurement M14 for three calendar years.
- Each Transmission Operator and Balancing Authority shall each keep data or evidence for each applicable Requirement R15 through R18, and Measure M15 through M18 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.
- Each Transmission Operator shall keep data or evidence for Requirement R20 and Measure M20 for the current calendar year and one previous calendar year.

- Each Transmission Operator shall keep evidence for Requirement R21 and Measure M21 for the most recent twelve calendar months, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.
- Each Balancing Authority shall keep data or evidence for Requirement R23 and Measure M23 for the current calendar year and one previous calendar year.
- Each Balancing Authority shall keep evidence for Requirement R24 and Measure M24 for the most recent twelve calendar months, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.

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 Transmission Operator failed to act to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.
R2.	N/A	N/A	N/A	The Balancing Authority failed to act to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions.
R3.	N/A	N/A	N/A	The responsible entity did not comply with an Operating Instruction issued by the Transmission Operator, and such action could have been physically implemented and would not have violated safety, equipment, regulatory, or statutory requirements.
R4.	N/A	N/A	N/A	The responsible entity did not inform its Transmission Operator of its inability to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				comply with an Operating Instruction issued by its Transmission Operator.
R5.	N/A	N/A	N/A	The responsible entity did not comply with an Operating Instruction issued by the Balancing Authority, and such action could have been physically implemented and would not have violated safety, equipment, regulatory, or statutory requirements.
R6.	N/A	N/A	N/A	The responsible entity did not inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority.
R7.	N/A	N/A	N/A	The Transmission Operator did not provide comparable assistance to other Transmission Operators within its Reliability Coordinator Area, when requested and able, and the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requesting entity had implemented its Emergency procedures, and such actions could have been physically implemented and would not have violated safety, equipment, regulatory, or statutory requirements.
R8.	The Transmission Operator did not inform one known impacted Transmission Operator or 5% or less of the known impacted Transmission Operators, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Transmission Operator Areas. OR, The Transmission Operator did not inform one known impacted	The Transmission Operator did not inform two known impacted Transmission Operators or more than 5% and less than or equal to 10% of the known impacted Transmission Operators, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Transmission Operator Areas. OR, The Transmission Operator did not inform two known impacted Balancing	The Transmission Operator did not inform three known impacted Transmission Operators or more than 10% and less than or equal to 15% of the known impacted Transmission Operators, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Transmission Operator Areas. OR, The Transmission Operator did not inform three known impacted Balancing	The Transmission Operator did not inform its Reliability Coordinator of its actual or expected operations that resulted in, or could have resulted in, an Emergency on those respective Transmission Operator Areas. OR The Transmission Operator did not inform four or more known impacted Transmission Operators or more than 15% of the known impacted Transmission Operators of its actual or expected

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Balancing Authorities or 5% or less of the known impacted Balancing Authorities, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.	Authorities or more than 5% and less than or equal to 10% of the known impacted Balancing Authorities, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.	Authorities or more than 10% and less than or equal to 15% of the known impacted Balancing Authorities, whichever is greater, of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.	operations that resulted in, or could have resulted in, an Emergency on those respective Transmission Operator Areas. OR, The Transmission Operator did not inform four or more known impacted Balancing Authorities or more than 15% of the known impacted Balancing Authorities of its actual or expected operations that resulted in, or could have resulted in, an Emergency on respective Balancing Authority Areas.
R9.	The responsible entity did not notify one known impacted interconnected entity or 5% or less of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30 minutes or more, for telemetering and control	The responsible entity did not notify two known impacted interconnected entities or more than 5% and less than or equal to 10% of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30	The responsible entity did not notify three known impacted interconnected entities or more than 10% and less than or equal to 15% of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30	The responsible entity did not notify its Reliability Coordinator of a planned outage, or an unplanned outage of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	OR, The responsible entity did not notify four or more known impacted interconnected entities or more than 15% of the known impacted entities, whichever is greater, of a planned outage, or an unplanned outage of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.
R10.	The Transmission Operator did not monitor, obtain, or utilize one of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	The Transmission Operator did not monitor, obtain, or utilize two of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	The Transmission Operator did not monitor, obtain, or utilize three of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	The Transmission Operator did not monitor, obtain, or utilize four or more of the items required or identified as necessary by the Transmission Operator and listed in Requirement R10 Part 10.1 through 10.6.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R11.	N/A	N/A	The Balancing Authority did not monitor the status of Remedial Action Schemes that impact generation or Load, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency.	The Balancing Authority did not monitor its Balancing Authority Area, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency.
R12.	N/A	N/A	N/A	The Transmission Operator exceeded an identified Interconnection Reliability Operating Limit (IROL) for a continuous duration greater than its associated IROL T_V.
R13.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for one 30-minute period within that 24-hour period.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for two 30-minute periods within that 24-hour period.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for three 30-minute periods within that 24-hour period.	For any sample 24-hour period within the 30-day retention period, the Transmission Operator's Real-time Assessment was not conducted for four or more 30-minute periods within that 24-hour period.
R14.	N/A	N/A	N/A	The Transmission Operator did not initiate its Operating

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Plan for mitigating a SOL exceedance identified as part of its Real-time monitoring or Real-time Assessment
R15.	N/A	N/A	N/A	The Transmission Operator did not inform its Reliability Coordinator of actions taken to return the System to within limits when a SOL had been exceeded.
R16.	N/A	N/A	N/A	The Transmission Operator did not provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.
R17.	N/A	N/A	N/A	The Balancing Authority did not provide its System Operators with the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.
R18.	N/A	N/A	N/A	The Transmission Operator failed to operate to the most limiting parameter in instances where there was a difference in SOLs.
R19. Reserved.				
R20.	N/A	N/A	The Transmission Operator had data exchange capabilities with its Reliability Coordinator, Balancing Authority, and identified entities for performing Real-time monitoring and Real-time Assessments, but did not have redundant and	The Transmission Operator did not have data exchange capabilities with its Reliability Coordinator, Balancing Authority, and identified entities for performing Real-time monitoring and Real-time Assessments as specified in the Requirement.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, as specified in the Requirement.	
R21.	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 90 calendar days but less than or equal to 120 calendar days since the previous test; OR The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 120 calendar days but less than or equal to 150 calendar days since the previous test; OR The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 150 calendar days but less than or equal to 180 calendar days since the previous test; OR The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality, but did so more than 180 calendar days since the previous test; OR The Transmission Operator did not test its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality; OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	but, following an unsuccessful test, initiated action to restore the redundant functionality in more than 2 hours and less than or equal to 4 hours.	redundant functionality in more than 4 hours and less than or equal to 6 hours.	redundant functionality in more than 6 hours and less than or equal to 8 hours.	The Transmission Operator tested its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, did not initiate action within 8 hours to restore the redundant functionality.
R22. Reserved.				
R23.	N/A	N/A	The Balancing Authority had data exchange capabilities with its Reliability Coordinator, Transmission Operator, and identified entities for performing Real-time monitoring and analysis functions, but did not have redundant and diversely routed data exchange infrastructure within the Balancing	The Balancing Authority did not have data exchange capabilities with its Reliability Coordinator, Transmission Operator, and identified entities for performing Real-time monitoring and analysis functions as specified in the Requirement.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Authority's primary Control Center, as specified in the Requirement.	
R24.	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 90 calendar days but less than or equal to 120 calendar days since the previous test; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in more than	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 120 calendar days but less than or equal to 150 calendar days since the previous test; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 150 calendar days but less than or equal to 180 calendar days since the previous test; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days but, following an unsuccessful test, initiated action to restore the redundant functionality in	The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality, but did so more than 180 calendar days since the previous test; OR The Balancing Authority did not test its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality; OR The Balancing Authority tested its primary Control Center data exchange capabilities specified in Requirement R23 for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	2 hours and less than or equal to 4 hours.	more than 4 hours and less than or equal to 6 hours.	more than 6 hours and less than or equal to 8 hours.	redundant functionality at least once every 90 calendar days but, following an unsuccessful test, did not initiate action within 8 hours to restore the redundant functionality.

D. Regional Variances

None.

E. Associated Documents

The Project 2014-03 SDT has created the SOL Exceedance White Paper as guidance on SOL issues and the URL for that document is: http://www.nerc.com/pa/stand/Pages/TOP0013RI.aspx.

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, including electronic data exchange, 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	November 1, 2006	Adopted by Board of Trustees	Revised
1a	May 12, 2010	Added Appendix 1 – Interpretation of R8 approved by Board of Trustees on May 12, 2010	Interpretation
1a	September 15, 2011	FERC Order issued approved the Interpretation of R8 (FERC Order became effective November 21, 2011)	Interpretation
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	February 12, 2015	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-001-3. Docket No. RM15-16-000. Order No. 817.	Approved
4	February 9, 2017	Adopted by Board of Trustees	Revised
4	April 17, 2017	FERC letter Order approved TOP-001-4. Docket No. RD17-4-000	
5	May 9, 2019	Adopted by Board of Trustees	R19 and R22 retired under Project 2018-03 Standards Efficiency Review Retirements
5	September 17, 2020	FERC Order issued approving TOP-001-5. Docket No. RM19-16-000, RM19-17-000	
5	December 14,2020		FERC Approval
5	April 1, 2021	Effective Date	

Guidelines and Technical Basis

None.

Rationale

Rationale text from the development of TOP-001-3 in Project 2014-03 and TOP-001-4 in Project 2016-01 follows. Additional information can be found on the Project 2014-03 and Project 2016-01 pages.

Rationale for Requirement R3:
The phrase 'cannot be physically implemented' means that a Transmission Operator may request something to be done that is not physically possible due to its lack of knowledge of the system involved.

Rationale for Requirement R10:
New proposed Requirement R10 is derived from approved IRO-003-2, Requirement R1, adapted to the Transmission Operator Area. This new requirement is in response to NOPR paragraph 60 concerning monitoring capabilities for the Transmission Operator. New Requirement R11 covers the Balancing Authorities. Monitoring of external systems can be accomplished via data links.

The revised requirement addresses directives for Transmission Operator (TOP) monitoring of some non-Bulk Electric System (BES) facilities as necessary for determining System Operating Limit (SOL) exceedances (FERC Order No. 817 Para 35-36). The proposed requirement corresponds with approved IRO-002-4 Requirement R4 (proposed IRO-002-5 Requirement R5), which specifies the Reliability Coordinator's (RC) monitoring responsibilities for determining SOL exceedances.

The intent of the requirement is to ensure that all facilities (i.e., BES and non-BES) that can adversely impact reliability of the BES are monitored. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. The facilities that are necessary for determining SOL exceedances should be either designated as part of the BES, or otherwise be incorporated into monitoring when identified by planning and operating studies such as the Operational Planning Analysis (OPA) required by TOP-002-4 Requirement R1 and IRO-008-2 Requirement R1. The SDT recognizes that not all non-BES facilities that a TOP considers necessary for its monitoring needs will need to be included in the BES.

The non-BES facilities that the TOP is required to monitor are only those that are necessary for the TOP to determine SOL exceedances within its Transmission Operator Area. TOPs perform various analyses and studies as part of their functional obligations that could lead to identification of non-BES facilities that should be monitored for determining SOL exceedances. Examples include:

- OPA;
- Real-time Assessments (RTA);

- Analysis performed by the TOP as part of BES Exception processing for including a facility in the BES; and
- Analysis which may be specified in the RC's outage coordination process that leads the TOP to identify a non-BES facility that should be temporarily monitored for determining SOL exceedances.

TOP-003-3 Requirement R1 specifies that the TOP shall develop a data specification which includes data and information needed by the TOP to support its OPAs, Real-time monitoring, and RTAs. This includes non-BES data and external network data as deemed necessary by the TOP.

The format of the proposed requirement has been changed from the approved standard to more clearly indicate which monitoring activities are required to be performed.

Rationale for Requirement R13:
The new Requirement R13 is in response to NOPR paragraphs 55 and 60 concerning Real-time analysis responsibilities for Transmission Operators and is copied from approved IRO-008-1, Requirement R2. The Transmission Operator's Operating Plan will describe how to perform the Real-time Assessment. The Operating Plan should contain instructions as to how to perform Operational Planning Analysis and Real-time Assessment with detailed instructions and timing requirements as to how to adapt to conditions where processes, procedures, and automated software systems are not available (if used). This could include instructions such as an indication that no actions may be required if system conditions have not changed significantly and that previous Contingency analysis or Real-time Assessments may be used in such a situation.

Rationale for Requirement R14:
The original Requirement R8 was deleted and original Requirements R9 and R11 were revised in order to respond to NOPR paragraph 42 which raised the issue of handling all SOLs and not just a sub-set of SOLs. The SDT has developed a white paper on SOL exceedances that explains its intent on what needs to be contained in such an Operating Plan. These Operating Plans are developed and documented in advance of Real-time and may be developed from Operational Planning Assessments required per proposed TOP-002-4 or other assessments. Operating Plans could be augmented by temporary operating guides which outline prevention/mitigation plans for specific situations which are identified day-to-day in an Operational Planning Assessment or a Real-time Assessment. The intent is to have a plan and philosophy that can be followed by an operator.

Rationale for Requirements R16 and R17:
In response to IERP Report recommendation 3 on authority.

Rationale for Requirement R18:
Moved from approved IRO-005-3.1a, Requirement R10. Transmission Service Provider, Distribution Provider, Load-Serving Entity, Generator Operator, and Purchasing-Selling Entity are deleted as those entities will receive instructions on limits from the responsible entities cited in the requirement. Note – Derived limits replaced by SOLs for clarity and specificity. SOLs include voltage, Stability, and thermal limits and are thus the most limiting factor.

Rationale for Requirements R19 and R20 (R19, R20, R22, and R23 in TOP-001-4):
[Note: Requirement R19 proposed for retirement under Project 2018-03 Standards Efficiency Review Retirements.]

The proposed changes address directives for redundancy and diverse routing of data exchange capabilities (FERC Order No. 817 Para 47).

Redundant and diversely routed data exchange capabilities consist of data exchange infrastructure components (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data) that will provide continued functionality despite failure or malfunction of an individual component within the Transmission Operator's (TOP) primary Control Center. Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. Requirement R20 does not require automatic or instantaneous fail-over of data exchange capabilities. Redundancy and diverse routing may be achieved in various ways depending on the arrangement of the infrastructure or hardware within the TOP's primary Control Center.

The reliability objective of redundancy is to provide for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

Infrastructure that is not within the TOP's primary Control Center is not addressed by the proposed requirement.

Rationale for Requirement R21:
The proposed requirement addresses directives for testing of data exchange capabilities used in primary Control Centers (FERC Order No. 817 Para 51).

A test for redundant functionality demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data). An entity's testing practices should, over time, examine the various failure modes of its data

exchange capabilities. When an actual event successfully exercises the redundant functionality, it can be considered a test for the purposes of the proposed requirement.

Rationale for Requirements R22 and R23:
[Note: Requirement R22 proposed for retirement under Project 2018-03 Standards Efficiency Review Retirements]

The proposed changes address directives for redundancy and diverse routing of data exchange capabilities (FERC Order No. 817 Para 47).

Redundant and diversely routed data exchange capabilities consist of data exchange infrastructure components (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data) that will provide continued functionality despite failure or malfunction of an individual component within the Balancing Authority's (BA) primary Control Center. Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. Requirement R23 does not require automatic or instantaneous fail-over of data exchange capabilities. Redundancy and diverse routing may be achieved in various ways depending on the arrangement of the infrastructure or hardware within the BA's primary Control Center.

The reliability objective of redundancy is to provide for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

Infrastructure that is not within the BA's primary Control Center is not addressed by the proposed requirement.

Rationale for Requirement R24:
The proposed requirement addresses directives for testing of data exchange capabilities used in primary Control Centers (FERC Order No. 817 Para 51).

A test for redundant functionality demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component(e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data). An entity's testing practices should, over time, examine the various failure modes of its data exchange capabilities. When an actual event successfully exercises the redundant functionality, it can be considered a test for the purposes of the proposed requirement.

A. Introduction

1. **Title: Operational Reliability Data**
2. **Number: TOP-003-5**
3. **Purpose:** To ensure that the Transmission Operator and Balancing Authority have data needed to fulfill their operational and planning responsibilities.
4. **Applicability:**
   - **4.1.** Transmission Operator
   - **4.2.** Balancing Authority
   - **4.3.** Generator Owner
   - **4.4.** Generator Operator
   - **4.5.** Transmission Owner
   - **4.6.** Distribution Provider
5. **Effective Date*:** See BC Implementation Plan for Project 2019-06.

B. Requirements and Measures

R1. Each Transmission Operator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **1.1.** A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data as deemed necessary by the Transmission Operator.
- **1.2.** Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.
- **1.3.** Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:
  - **1.3.1.** Operating limitations based on:
    - **1.3.1.1.** capability and availability;
    - **1.3.1.2.** fuel supply and inventory concerns;
    - **1.3.1.3.** fuel switching capabilities; and
    - **1.3.1.4.** environmental constraints
  - **1.3.2.** Generating unit(s) minimum:
    - **1.3.2.1.** design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. A periodicity for providing data.

1.5. The deadline by which the respondent is to provide the indicated data.

M1. Each Transmission Operator shall make available its dated, current, in force documented specification for data.

R2. Each Balancing Authority shall maintain a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. A list of data and information needed by the Balancing Authority to support its analysis functions and Real-time monitoring.

2.2. Provisions for notification of current Protection System and Remedial Action Scheme status or degradation that impacts System reliability.

2.3. Provisions for notification of BES generating unit(s) status during local forecasted cold weather to include:

2.3.1. Operating limitations based on:

2.3.1.1. capability and availability;

2.3.1.2. fuel supply and inventory concerns;

2.3.1.3. fuel switching capabilities; and

2.3.1.4. environmental constraints.

2.3.2. Generating unit(s) minimum:

2.3.2.1. design temperature; or

2.3.2.2. historical operating temperature; or

2.3.2.3. current cold weather performance temperature determined by an engineering analysis.

2.4. A periodicity for providing data.

2.5. The deadline by which the respondent is to provide the indicated data.

M2. Each Balancing Authority shall make available its dated, current, in force documented specification for data.

R3. Each Transmission Operator shall distribute its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M3. Each Transmission Operator shall make available evidence that it has distributed its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R4. Each Balancing Authority shall distribute its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Each Balancing Authority shall make available evidence that it has distributed its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, or e-mail records.

R5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall satisfy the obligations of the documented specifications using: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

5.1. A mutually agreeable format

5.2. A mutually agreeable process for resolving data conflicts

5.3. A mutually agreeable security protocol

M5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations of the documented specifications. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
The British Columbia Utilities Commission.

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.

Each responsible entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

Each Transmission Operator shall retain its dated, current, in force, documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.

Each Balancing Authority shall retain its dated, current, in force, documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring in accordance with Requirement R2 and Measurement M2 as well as any documents in force since the last compliance audit.

Each Transmission Operator shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.

Each Balancing Authority shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring in accordance with Requirement R4 and Measurement M4.

Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R5 and Measurement M5.

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 #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Transmission Operator did not include two or fewer of the parts (Part 1.1 through Part 1.5) 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 1.5) 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 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include any of the parts (Part 1.1 through Part 1.5) 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	Lower	The Balancing Authority did not include two or fewer of the parts (Part 2.1 through Part 2.5) 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 2.5) 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 2.5) 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 any of the parts (Part 2.1 through Part 2.5) 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	Lower	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	Lower	The Balancing Authority did not distribute its data specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to two entities, or more than 5% and less than or equal to 10% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to three entities, or more than 10% and less than or equal to 15% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to four or more entities, or more than 15% of the entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring.

TOP-003-5 — Operational Reliability Data

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

BC Implementation Plan for Project 2019-06.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP-003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
4	June 11, 2021	Board approved	Project 2019-06 Cold Weather

4	August 24, 2021	FERC approved TOP –003-5 Docket No. RD21-5-000, Order	
4	August 24, 2021	April 1, 2023	Effective Date