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-33-18

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. 11

BEFORE:
W. M. Everett, QC, Commissioner

on September 27, 2018

ORDER

WHEREAS:

A. On May 1, 2018, the British Columbia Hydro and Power Authority (BC Hydro) filed Mandatory Reliability Standards (MRS) Assessment Report No. 11 (Report No. 11) with the British Columbia Utilities Commission (BCUC), assessing two new standards and ten revised standards (collectively, Revised Standards) and one retired standard (Retired Standard) developed by the North American Electric Reliability Corporation (NERC) and/or the Western Electricity Coordinating Council (WECC). In MRS Report No. 11, BC Hydro has assessed reliability standards that were Federal Energy Regulatory Commission (FERC) approved with an effective order within the period between, and including, December 1, 2016 and November 30, 2017;

B. The Revised Standards assessed by BC Hydro in MRS Report No. 11 are based on defined terms contained in the NERC Glossary of Terms Used in Reliability Standards dated October 6, 2017 (NERC Glossary). In addition, BC Hydro assessed nine new defined terms (Revised Terms) and four retired defined terms (Retired Terms) contained in the NERC Glossary. MRS Report No. 11 recommends the nine Revised Terms and four Retired Terms be adopted and retired respectively by the BCUC as they will preserve or enhance the reliability of the Bulk Electric System in BC, and thus serve the public interest;

C. In MRS Report No. 11, BC Hydro recommends that eleven of the twelve Revised Standards and all nine Revised Terms are suitable for adoption in BC at this time. In addition, BC Hydro recommends one Retired Standard and four Retired Terms are suitable for retirement in BC;

D. To date, BC Hydro states it has acted as the Planning Authority/Planning Coordinator (PA/PC) for the BC Hydro asset footprint only. The functional registration of the PA/PC role for the entire Province of BC remains outstanding. Revised Standard PRC-012-2 (Attachment 1, Section II Parts 6(d) and 6(e) referenced in Requirement R1; Attachment 2, Section I Parts 7(d) and 7(e) referenced in Requirement R2; and Requirement R4) and Revised Standard PRC-006-3 are considered in MRS Report No. 11 and contain requirements that pertain to the PC function. BC Hydro recommends the aforementioned sections of

Revised Standard PRC-012-2 and Revised Standard PRC-006-3, pertaining to the PC function, be held in abeyance and be of no force or effect in BC until the PC function is resolved;

E. BC Hydro recommends that, in connection with the adoption of IRO-002-5, TOP-001-4 and applicable sections of PRC-012-2, BC-specific versions of the FERC approved related Implementation Plans be adopted in BC. BC Hydro provided BC-specific versions of the IRO-002-5/TOP-001-4 Implementation Plan and PRC-012-2 Implementation Plan as part of MRS Report No. 11 for the BCUC's consideration;

F. On May 25, 2018, BC Hydro filed Errata No. 1 to MRS Report No. 11. BC Hydro submits that CIP-003-5 Requirements R2.2 and R2.3 be held in abeyance until CIP-003-7 has been assessed at a later date;

G. By Order R-26-18 dated June 13, 2018, BC Hydro was directed to publish a notice of process for MRS Report No. 11 and the Regulatory Timetable was established for public comment;

H. On June 29, 2018, FortisBC Inc. submitted that its comments are reflected in BC Hydro's MRS Report No. 11 and that it had no additional comments;

I. On July 26, 2018, the BCUC issued information requests (IRs) to BC Hydro in response to MRS Report No. 11 and on August 17, 2018, BC Hydro submitted its IR responses;

J. The BCUC did not review the recoverability of the estimated costs to adopt the Revised Standards, Retired Standard, Revised Terms and Retired Terms;

K. Although not assessed by BC Hydro, the BCUC considers that the Compliance Provisions of the reliability standards should be adopted to maintain compliance monitoring consistency with other jurisdictions that have adopted the reliability standards with the Compliance Provisions. The BCUC finds it appropriate to provide effective dates for BC entities to come into compliance with the Revised Standards and Revised Terms adopted in this order;

L. Pursuant to section 125.2(6) of the *Utilities Commission Act*, the BCUC must adopt the reliability standards addressed in MRS Report No. 11 if the BCUC considers that the reliability standards are required to maintain or achieve consistency in BC with other jurisdictions that have adopted the reliablity standards; and

M. The BCUC has reviewed and considered MRS Report No. 11, the Revised Standards, Retired Standard, Revised Terms and Retired Terms assessed therein, comments received from entities and the responses to IRs and considers that the adoption of the recommendations in MRS Report No. 11 is warranted.

NOW THEREFORE pursuant to section 125.2 of the *Utilities Commission Act*, which provides the BCUC exclusive jurisdiction to determine whether a reliability standard is in the public interest and should be adopted in BC, the BCUC orders as follows:

1. Eleven of the twelve Revised Standards assessed in MRS Report No. 11 are adopted with effective dates in Table 1 of Attachment A to this order and 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. All reliability standards listed in Attachment B to this order are in effect 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. Attachment B to this order also includes those reliability standards with retirement/effective dates held in abeyance to be assessed at a later date.

3. 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.

4. The NERC Glossary is adopted to define terms employed in the reliability standards. The effective date of each of the new or Revised Terms adopted and the date of each Retired Term is the date in Table 2 of Attachment A to this order. Each glossary term to be superseded by a Revised Term adopted in this order shall remain in effect until the effective date of the Revised Term superseding it.

5. The Revised Terms listed in Attachment C to this order are in effect in BC as of the effective dates indicated. The effective dates for the Revised Terms listed in Attachment C supersede the effective dates that were included in any similar list appended to any previous order. Other terms in the NERC Glossary, which do not include a United States FERC approval date on or before November 30, 2017, are of no force or effect in BC.

6. 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.

7. Revised Standard PRC-012-2 (Attachment 1, Section II Parts 6(d) and 6(e) referenced in Requirement R1; Attachment 2, Section I Parts 7(d) and 7(e) referenced in Requirement R2; and Requirement R4) and Revised Standard PRC-006-3, considered in MRS Report No. 11 and containing PC function requirements, are to be held in abeyance and are of no force or effect in BC.

8. The BC-specific versions of the IRO-002-5/TOP-001-4 Implementation Plan and the PRC-012-2 Implementation Plan are adopted in the form directed by the BCUC and as amended from time to time, and effective in BC as indicated in Attachment D to this order. The BC-specific versions of the IRO-002-5/TOP-001-4 Implementation Plan and PRC-012-2 Implementation Plan will be posted on the WECC website with links from the BCUC website.

9. CIP-003-5 Requirements R2.2 and R2.3 are held in abeyance until CIP-003-7 has been assessed at a later date.

10. The Revised Standards in their written form are adopted as set out in Attachment E to this order.

11. The reliability standards adopted in BC will be posted on the WECC website with a link from the BCUC website.

12. Entities subject to Mandatory Reliability Standards are required to report to the BCUC and may, on a voluntary basis, report to NERC as an Electric Reliability Organization or to FERC.

DATED at the City of Vancouver, in the Province of British Columbia, this 27th day of September 2018.

BY ORDER

Original Signed By:

W. M. Everett, QC
Commissioner

Attachments

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-005-1	Balancing Authority Control	October 1, 2019	Revised	BAL-005-0.2b BAL-006-2 Requirement R3
2.	CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	October 1, 2018	Revised	CIP-002-5.1
3.	FAC-001-3	Facility Interconnection Requirements	October 1, 2019	Revised	FAC-001-2
4.	IRO-002-5	Reliability Coordination – Monitoring and Analysis	January 1, 2019 See BC IRO-002-5/TOP-001-4 Implementation Plan.	Revised	IRO-002-4
5.	IRO-018-1(i)	Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities	April 1, 2020	Revised	IRO-018-1
6.	PRC-006-3	Automatic Underfrequency Load Shedding	To be determined. Unable to be assessed at this time.	New	PRC-007-0 PRC-009-0
7.	PRC-012-2	Remedial Action Schemes	October 1, 2021 See BC PRC-012-2 Implementation Plan. **R1**: Attachment 1, Section II Parts 6(d) and 6(e) to be determined. Unable to be assessed at this time. **R2**: Attachment 2, Section I Parts 7(d) and 7(e) to be determined. Unable to be assessed at this time. **R4**: To be determined. Unable to be assessed at this time.	New	PRC-015-1 PRC-016-1

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

	Standard	Standard Name	Effective Date	Type	BCUC Approved Standard(s) Being Superseded[1]
8.	TOP-001-4	Transmission Operations	October 1, 2020 See BC IRO-002-5/TOP-001-4 Implementation Plan.	Revised	TOP-001-3
9.	TOP-007-WECC-1a	System Operating Limits	October 1, 2018	Retired	N/A
10.	TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities	October 1, 2020	Revised	TOP-010-1
11.	VAR-001-4.2	Voltage and Reactive Control	October 1, 2018	Revised	VAR-001-4.1
12.	VAR-002-4.1	Generator Operation for Maintaining Network Voltage Schedules	October 1, 2018	Revised	VAR-002-4
13.	VAR-501-WECC-3.1	Power System Stabilizer (PSS)	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.	Revised	VAR-501-WECC-2

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

Table 2 British Columbia Utilities Commission NERC Glossary Terms with Effective Dates as Adopted

	NERC Glossary Term	Acronym	Effective Date	BCUC Approved Term to be Replaced or Retired
1	Actual Frequency (F_A)	N/A	October 1, 2019	New Term
2	Actual Net Interchange (NI_A)	N/A	October 1, 2019	New Term
3	Automatic Time Error Correction (I_{ATEC})	N/A	October 1, 2019	New Term
4	Interchange Meter Error (I_{ME})	N/A	October 1, 2019	New Term
5	Reporting ACE	N/A	October 1, 2019	Reporting ACE
6	Scheduled Net Interchange (NI_S)	N/A	October 1, 2019	New Term
7	Automatic Generation Control	AGC	October 1, 2019	Automatic Generation Control
8	Balancing Authority	N/A	January 1, 2019	Balancing Authority
9	Disturbance	N/A	October 1, 2018	Retired (WECC regional term)
10	Energy Emergency	N/A	October 1, 2018	Retired
11	Non-Spinning Reserve	N/A	October 1, 2018	Retired (WECC regional term)
12	Pseudo-Tie	N/A	January 1, 2019	Pseudo-Tie
13	Spinning Reserve	N/A	October 1, 2018	Retired (WECC regional term)

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-002-2	Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event	R-39-17	January 1, 2018
BAL-002-WECC-2a	Contingency Reserve	R-39-17	July 26, 2017
BAL-003-1.1	Frequency Response and Frequency Bias Setting	R-32-16A	October 1, 2016
BAL-004-0	Time Error Correction	G-67-09	November 1, 2010
BAL-004-WECC-2	Automatic Time Error Correction	R-32-14	October 1, 2014
BAL-005-0.2b[1]	Automatic Generation Control	R-41-13	December 12, 2013 R2: Retired January 21, 2014[2]
BAL-005-1	Balancing Authority Control	R-33-18	October 1, 2019
BAL-006-2[3]	Inadvertent Interchange	R-1-13	April 15, 2013
CIP-002-3[1]	Cyber Security – Critical Cyber Asset Identification	G-162-11	July 1, 2012
CIP-002-5.1[1]	Cyber Security – BES Cyber System Categorization	R-38-15	October 1, 2018
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	R-33-18	October 1, 2018
CIP-003-3[1, 4, 5]	Cyber Security – Security Management Controls	G-162-11	July 1, 2012 R1.2, R3, R3.1, R3.2, R3.3, R4.2: Retired January 21, 2014[2]
CIP-003-5[1]	Cyber Security – Security Management Controls	R-38-15	October 1, 2018 R2.2, R2.3: Adoption held in abeyance pending the adoption of CIP-003-7.

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 On November 21, 2013, FERC Order 788 (referred to as Paragraph 81) approved the retiring of the reliability standard requirements.
3 Reliability standard is superseded by BAL-005-1 as of the BAL-005-1 effective date.
4 Reliability standard is superseded by CIP-010-1 as of the CIP-010-1 effective date.
5 Reliability standard is superseded by CIP-011-1 as of the CIP-011-1 effective date.

Standard	Name	BCUC Order Adopting	Effective Date
CIP-003-6	Cyber Security — Security Management Controls	n/a	Adoption held in abeyance at this time[6]
CIP-004-3a[1]	Cyber Security - Personnel & Training	R-32-14	August 1, 2014
CIP-004-6	Cyber Security — Personnel & Training	R-39-17	October 1, 2018
CIP-005-3a[1, 4]	Cyber Security – Electronic Security Perimeter(s)	R-1-13	July 15, 2013 R2.6: Retired January 21, 2014[2]
CIP-005-5	Cyber Security – Electronic Security Perimeter(s)	R-38-15	October 1, 2018
CIP-006-3c[1]	Cyber Security – Physical Security of Critical Cyber Assets	G-162-11	July 1, 2012
CIP-006-6	Cyber Security — Physical Security of BES Cyber Systems	R-39-17	October 1, 2018
CIP-007-3a[1, 4, 5]	Cyber Security - Systems Security Management	R-32-14	August 1, 2014 R7.3: Retired January 21, 2014[2]
CIP-007-6	Cyber Security — System Security Management	R-39-17	October 1, 2018
CIP-008-3[1]	Cyber Security – Incident Reporting and Response Planning	G-162-11	July 1, 2012
CIP-008-5	Cyber Security – Incident Reporting and Response Planning	R-38-15	October 1, 2018
CIP-009-3[1]	Cyber Security – Recovery Plans for Critical Cyber Assets	G-162-11	July 1, 2012
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	R-39-17	October 1, 2018
CIP-010-2	Cyber Security – Configuration Change Management and Vulnerability Assessments	R-39-17	October 1, 2018
CIP-011-2	Cyber Security – Information Protection	R-39-17	October 1, 2018
CIP-014-2	Physical Security	R-32-16A	October 1, 2017 and as per BC-specific Implementation Plan
COM-001-2.1[1]	Communications	R-32-16A	October 1, 2017
COM-001-3	Communications	R-39-17	R1, R2: October 1, 2017 R3–R13: October 1, 2018
COM-002-4	Operating Personnel Communications Protocols	R-32-16A	April 1, 2017
EOP-001-2.1b[7]	Emergency Operations Planning	R-32-14	August 1, 2014
EOP-002-3.1[7]	Capacity and Energy Emergencies	R-32-14	August 1, 2014

[6] BC Hydro recommends that the CIP-003-6 reliability standard be held in abeyance and be of no force or effect in BC due to technical suitability issues that will not improve reliability and instead place undue burden on responsible entities. When adopted by FERC, the NERC approved CIP-003-7 reliability standard will retire CIP-003-6. CIP-003-7 will be assessed in the next MRS Assessment Report.

[7] Reliability standard is superseded by EOP-011-1 as of the EOP-011-1 effective date.

Standard	Name	BCUC Order Adopting	Effective Date
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-004-3	Event Reporting	R-39-17	October 1, 2017
EOP-005-2	System Restoration and Blackstart Resources	R-32-14	August 1, 2015 R3.1: Retired January 21, 2014[2]
EOP-006-2	System Restoration Coordination	R-32-14	August 1, 2014
EOP-008-1	Loss of Control Center Functionality	R-32-14	August 1, 2015
EOP-010-1[11]	Geomagnetic Disturbance Operations	R-38-15	R1, R3: October 1, 2016 R2: At retirement of IRO-005-3.1a R3
EOP-011-1	Emergency Operations	R-39-17	October 1, 2018
FAC-001-2[1]	Facility Interconnection Requirements	R-38-15	October 1, 2016
FAC-001-3	Facility Interconnection Requirements	R-33-18	October 1, 2019
FAC-002-2	Facility Interconnection Studies	R-38-15	October 1, 2015
FAC-003-4	Transmission Vegetation Management	R-39-17	October 1, 2017
FAC-501-WECC-1	Transmission Maintenance	R-1-13	April 15, 2013
FAC-008-3	Facility Ratings	R-32-14	August 1, 2015 R4, R5: Retired January 21, 2014[2]
FAC-010-3	System Operating Limits Methodology for the Planning Horizon	R-39-17	R1–R4: October 1, 2017 R5: Retired
FAC-011-3	System Operating Limits Methodology for the Operations Horizon	R-39-17	October 1, 2017
FAC-013-1[12]	Establish and Communicate Transfer Capability	G-67-09	November 1, 2010
FAC-013-2	Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon	n/a	Adoption held in abeyance at this time[10]
FAC-014-2	Establish and Communicate System Operating Limits	G-167-10	January 1, 2011

[8] Reliability standard would be superseded by EOP-003-2 if adopted in BC. 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 R1 if adopted in BC. Adoption of PRC-010-2 pending reassessment.

[10] Unable to assess based on undefined Planning Coordinator/Planning Authority footprints and entities responsible. The BCUC reasons for decision appended to Order R-41-13 (page 20), indicated that a separate process would be established to consider this matter as it pertains to BC.

[11] Requirement R2 of the reliability standard will be effective upon the retirement of IRO-005-3.1a Requirement R3 which follows the effective date of IRO-002-4.

[12] Reliability standard would be superseded by the FAC-013-2 if adopted in BC. Adoption of FAC-013-2 pending reassessment.

Standard	Name	BCUC Order Adopting	Effective Date
INT-004-3.1	Dynamic Transfers	R-38-15	R1, R2: October 1, 2015 R3: January 1, 2016
INT-006-4	Evaluation of Interchange Transactions	R-38-15	October 1, 2015
INT-009-2.1	Implementation of Interchange	R-38-15	October 1, 2015
INT-010-2.1	Interchange Initiation and Modification for Reliability	R-38-15	October 1, 2015
INT-011-1.1	Intra-Balancing Authority Transaction Identification	R-38-15	October 1, 2015
IRO-001-4	Reliability Coordination – Responsibilities	R-39-17	October 1, 2017
IRO-002-2[13]	Reliability Coordination – Facilities	R-1-13	April 15, 2013
IRO-002-4[1]	Reliability Coordination – Monitoring and Analysis	R-39-17	October 1, 2017
IRO-002-5	Reliability Coordination – Monitoring and Analysis	R-33-18	January 1, 2019
IRO-003-2[13]	Reliability Coordination – Wide Area View	G-67-09	November 1, 2010
IRO-004-2[13]	Reliability Coordination – Operations planning	R-1-13	April 15, 2013
IRO-005-3.1a[13,14]	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-2	Qualified Transfer Path Unscheduled Flow (USF) Relief	R-38-15	October 1, 2015
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-010-1a[13]	Reliability Coordinator Data Specification and Collection	R-1-13	April 15, 2013
IRO-010-2	Reliability Coordinator Data Specification and Collection	R-39-17	April 1, 2019
IRO-014-1[13]	Procedures, Processes, or Plans to Support Coordination Between Reliability coordinators	G-67-09	November 1, 2010
IRO-014-3	Coordination Among Reliability Coordinators	R-39-17	October 1, 2017
IRO-015-1[13]	Notification and Information Exchange	G-67-09	November 1, 2010
IRO-017-1	Outage Coordination	R-39-17	October 1, 2020

[13] Refer to "IRO and TOP Reliability Standards Supersession Mapping" section below.
[14] Requirement R3 of the reliability standard is superseded by EOP-010-1 Requirement R2 as of the IRO-002-4 effective date.

Standard	Name	BCUC Order Adopting	Effective Date
IRO-018-1[1]	Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities	R-39-17	April 1, 2018
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[15]	Steady-State Data for Modeling and Simulation for the Interconnected Transmission System	G-67-09	November 1, 2010
MOD-012-0[15]	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
MOD-025-2	Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability	R-38-15	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by October 1, 2020
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-031-2	Demand and Energy Data	R-39-17	April 1, 2018
MOD-032-1	Data for Power System Modeling and Analysis	R-38-15	Effective date held in abeyance[10]
MOD-033-1	Steady-State and Dynamic System Model Validation	R-38-15	Effective date held in abeyance[10]

[15] Reliability standard will be superseded by MOD-032-1 and MOD-033-1 if adopted in BC. Adoption of MOD-032-1 and MOD-033-1 pending reassessment.

Standard	Name	BCUC Order Adopting	Effective Date
NUC-001-3	Nuclear Plant Interface Coordination	R-38-15	January 1, 2016
PER-001-0.2[13]	Operating Personnel Responsibility and Authority	R-41-13	December 12, 2013
PER-002-0	Operating Personnel Training	G-67-09	November 1, 2010
PER-003-1	Operating Personnel Credentials	R-41-13	January 1, 2015
PER-004-2	Reliability Coordination – Staffing	R-1-13	January 15, 2013
PER-005-2	Operations Personnel Training	R-38-15	R1–R4, R6: October 1, 2016 R5: October 1, 2017
PRC-001-1.1(ii)	System Protection Coordination	R-32-16A	October 1, 2016
PRC-002-2	Disturbance Monitoring and Reporting Requirements	R-32-16A	R1, R5: April 1, 2017 R2–R4, R6–R11: staged as per BC-specific Implementation Plan R12: July 1, 2017
PRC-004-5(i)	Protection System Misoperation Identification and Correction	R-32-16A	October 1, 2017
PRC-004-WECC-2	Protection System and Remedial Action Scheme Misoperation	R-39-17	October 1, 2017
PRC-005-1.1b[1, 18]	Transmission and Generation Protection System Maintenance and Testing	R-32-14	January 1, 2015
PRC-005-2[1]	Protection System Maintenance	R-38-15	R1, R2, R5: October 1, 2017 R3, R4: staged as per BC-specific Implementation Plan
PRC-005-2(i)[1]	Protection System Maintenance	R-32-16A	R1, R2, R5: October 1, 2017 R3, R4: staged as per BC-specific Implementation Plan
PRC-005-6	Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance	R-39-17	R1, R2, R5: October 1, 2019 R3, R4: See Implementation Plan
PRC-006-2[1,16]	Automatic Underfrequency Load Shedding		Adoption held in abeyance at this time[10]
PRC-006-3	Automatic Underfrequency Load Shedding	R-33-18	Adoption held in abeyance at this time
PRC-007-0[17]	Assuring consistency of entity Underfrequency Load Shedding Program Requirements	G-67-09	November 1, 2010
PRC-008-0[18]	Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program	G-67-09	November 1, 2010

[16] Reliability standard supersedes PRC-006-1 which has been held in abeyance due to the undefined Planning Coordinator/Planning Authority footprints and entities responsible.
[17] Reliability standard will be superseded by PRC-006-2 if adopted in BC. Adoption of PRC-006-2 pending reassessment.
[18] Reliability standard is superseded by PRC-005-6 as per the PRC-005-6 BC-specific Implementation Plan.

Standard	Name	BCUC Order Adopting	Effective Date
PRC-009-0[17]	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[2]
PRC-010-2	Under Voltage Load Shedding		Adoption held in abeyance at this time[10]
PRC-011-0[18]	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. Unable to be assessed at this time. R2: Attachment 2, Section I Parts 7(d) and 7(e) to be determined. Unable to be assessed at this time. R4: To be determined. Unable to be assessed at this time.
PRC-015-1[19]	Remedial Action Scheme Data and Documentation	R-39-17	October 1, 2017
PRC-016-1[19]	Remedial Action Scheme Misoperations	R-39-17	October 1, 2017
PRC-017-1[18]	Remedial Action Scheme Maintenance and Testing	R-39-17	October 1, 2017
PRC-018-1[20]	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	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by October 1, 2020
PRC-021-1[21]	Under Voltage Load Shedding Program Data	G-67-09	November 1, 2010
PRC-022-1[21]	Under Voltage Load Shedding Program Performance	G-67-09	November 1, 2010 R2: Retired January 21, 2014[2]

19 Reliability standard is superseded by PRC-012-2 as of the PRC-012-2 effective date.
20 Reliability standard is superseded by PRC-002-2 as of the PRC-002-2 effective date.
21 Reliability standard is superseded by PRC-010-2 if adopted in BC. Adoption of PRC-010-2 pending reassessment.

Standard	Name	BCUC Order Adopting	Effective Date
PRC-023-2[1, 22]	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-025-1 R1 is completely effective in BC. 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
PRC-024-2	Generator Frequency and Voltage Protective Relay Settings	R-32-16A	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by October 1, 2020
PRC-025-1	Generator Relay Loadability	R-38-15	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by October 1, 2020
PRC-026-1	Relay Performance During Stable Power Swings	n/a	Adoption held in abeyance at this time[10]
TOP-001-1a[13]	Reliability Responsibilities and Authorities	R-1-13	January 15, 2013
TOP-001-3[1]	Transmission Operations	R-39-17	October 1, 2020
TOP-001-4	Transmission Operations	R-33-18	October 1, 2020
TOP-002-2.1b[13]	Normal Operations Planning	R-41-13	December 12, 2013
TOP-002-4	Operations Planning	R-39-17	October 1, 2020
TOP-003-1[13]	Planned Outage Coordination	R-1-13	April 15, 2013
TOP-003-3	Operational Reliability Data	R-39-17	April 1, 2019
TOP-004-2[13]	Transmission Operations	G-167-10	January 1, 2011
TOP-005-2a[13]	Operational Reliability Information	R-1-13	April 15, 2013
TOP-006-2[13]	Monitoring System Conditions	R-1-13	April 15, 2013

[22] PRC-023-2 Requirement R1, Criterion 6 only is superseded by PRC-025-1 as of PRC-025-1's 100 percent effective date.

Standard	Name	BCUC Order Adopting	Effective Date
TOP-007-0[13]	Reporting System Operating Unit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations	G-67-09	November 1, 2010
TOP-007-WECC-1a[23]	System Operating Limits	R-38-15	October 1, 2015 All Requirements Retired: October 1, 2018
TOP-008-1[13]	Response to Transmission Limit Violations	G-67-09	November 1, 2010
TOP-010-1[1]	Real-time Reliability Monitoring and Analysis Capabilities	R-39-17	October 1, 2020
TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities	R-33-18	October 1, 2020
TPL-001-0.1[24]	System Performance Under Normal (No Contingency) Conditions (Category A)	G-167-10	January 1, 2011
TPL-001-4	Transmission System Planning Performance Requirements	R-27-18A	R1: July 1, 2019 R2–R6, R8: July 1, 2020 R7: TBD[10]
TPL-002-0b[24]	System Performance Following Loss of a Single Bulk Electric System Element (Category B)	R-1-13	January 15, 2013
TPL-003-0b[24]	System Performance Following Loss of Two or More Bulk Electric System Elements (Category C)	R-32-14	August 1, 2014
TPL-004-0a[24]	System Performance Following Extreme Events Resulting in the Loss of Two or More Bulk Electric System Elements (Category D)	R-32-14	August 1, 2014
TPL-007-1	Transmission System Planned Performance for Geomagnetic Disturbance Events	n/a	Adoption held in abeyance at this time[10]
VAR-001-4.1[1]	Voltage and Reactive Control	R-32-16A	October 1, 2016
VAR-001-4.2	Voltage and Reactive Control	R-33-18	October 1, 2018
VAR-002-4[1]	Generator Operation for Maintaining Network Voltage Schedules	R-32-16A	October 1, 2016
VAR-002-4.1	Generator Operation for Maintaining Network Voltage Schedules	R-33-18	October 1, 2018
VAR-002-WECC-2	Automatic Voltage Regulators (AVR)	R-32-16A	October 1, 2016
VAR-501-WECC-2[1]	Power System Stabilizer (PSS)	R-32-16A	October 1, 2016

[23] Reliability Standard TOP-007-WECC-1a is to be retired.
[24] Reliability standard will be superseded by TPL-001-4 Requirements R2–R6 and R8 as of their effective dates.

Standard	Name	BCUC Order Adopting	Effective Date
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 pior 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, TOP and PER reliability standards by the revised/replacement IRO and TOP reliability standards adopted or yet to be adopted in BC as of the effective date in the "BC Reliability Standards" section above:

IRO-001-1.1	-	Reliability Coordination - Responsibilities and Authorities
IRO-002-2	-	Reliability Coordination - Facilities
IRO-003-2	-	Reliability Coordination - Wide-Area View
IRO-004-2	-	Reliability Coordination - Operations Planning
IRO-005-3.1a	-	Reliability Coordination - Current Day Operations
IRO-008-1	-	Reliability Coordinator Operational Analyses and Real-time Assessments
IRO-010-1a	-	Reliability Coordinator Data Specification and Collection
IRO-014-1	-	Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators
IRO-015-1	-	Notifications and Information Exchange Between Reliability Coordinators
IRO-016-1	-	Coordination of Real-time Activities Between Reliability Coordinators
PER-001-0.2	-	Operating Personnel Responsibility and Authority
TOP-001-1a	-	Reliability Responsibilities and Authorities
TOP-002-2.1b	-	Normal Operations Planning
TOP-003-1	-	Planned Outage Coordination
TOP-004-2	-	Transmission Operations
TOP-005-2a	-	Operational Reliability Information
TOP-006-2	-	Monitoring System Conditions
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-001-1.1 — Reliability Coordination - Responsibilities and Authorities	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirements R1–R6, R8 and R9	IRO-001-4
Requirement R7	IRO-014-3

Standard IRO-002-2 — Reliability Coordination - Facilities	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirements R1, R3–R5, R7 and R8	IRO-002-4
Requirement R2	IRO-010-2
Requirement R6	IRO-008-2

Standard IRO-003-2 — Reliability Coordination - Wide-Area View	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
All Requirements	IRO-002-4

Standard IRO-004-2 — Reliability Coordination - Operations Planning	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
All Requirements	IRO-001-4 IRO-008-2

Standard IRO-005-3.1a — Reliability Coordination - Current Day Operations	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirements R1–R3	IRO-002-4
Requirement R4	IRO-008-2
Requirements R5 and R8	IRO-001-4 IRO-002-4
Requirements R6 and R7	IRO-008-2 IRO-017-1
Requirement R8	IRO-001-4 IRO-002-4
Requirement R9	IRO-002-4 IRO-010-2
Requirement R10	IRO-009-1 TOP-001-3
Requirement R11	MOD-001-2, Requirement R2 (pending FERC adoption in the US and subsequent assessment and adoption in BC)
Requirement R12	IRO-008-2

Standard IRO-008-1 — Reliability Coordination - Current Day Operations	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
All Requirements	IRO-008-2

Standard IRO-010-1a — Reliability Coordinator Data Specification and Collection	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
All Requirements	IRO-010-2

Standard IRO-014-1 — Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirement R1	IRO-014-3 IRO-010-2
Requirements R2–R4	IRO-014-3

Standard IRO-015-1 — Notifications and Information Exchange Between Reliability Coordinators	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirements R1 and R2	IRO-014-3
Requirement R3	IRO-010-2

Standard IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
All Requirements	IRO-014-3

Standard PER-001-0.2 — Operating Personnel Responsibility and Authority	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
All Requirements	TOP-001-3

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

Standard TOP-002-2.1b — Normal Operations Planning	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirement R1	TOP-001-3 TOP-002-4
Requirements R2, R5–R9 and R12	TOP-002-4
Requirement R3	IRO-017-1 TOP-003-3
Requirement R4	IRO-017-1 IRO-008-2
Requirement R10	IRO-017-1 TOP-001-3 TOP-002-4 TOP-003-3
Requirement R11	TOP-001-3 TOP-002-4
Requirement R13	TOP-001-3 TOP-003-3
Requirements R14, R15 and R19	TOP-003-3
Requirements R16, R17 and R18	IRO-010-2

Standard TOP-003-1 — Planned Outage Coordination	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirement R1	IRO-010-2 TOP-003-3
Requirement R2	IRO-017-1 TOP-003-3
Requirement R3	TOP-001-3
Requirement R4	IRO-008-2 IRO-017-1

Standard TOP-004-2 — Transmission Operations	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirement R1	TOP-001-3
Requirement R2	TOP-001-3 TOP-002-4
Requirements R3 and R4	TOP-001-3
Requirement R5	Retired
Requirement R6	IRO-017-1 TOP-001-3

Standard TOP-005-2a — Operational Reliability Information	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirement R1	IRO-010-2 TOP-003-3
Requirement R2	TOP-003-3
Requirement R3	Retired

Standard TOP-006-2 — Monitoring System Conditions	
Requirement Being Superseded	**Superseding BCUC Approved Standard(s)**
Requirement R1	IRO-010-2 TOP-001-3 TOP-003-3
Requirement R2	IRO-002-4 TOP-001-3
Requirement R3	IRO-010-2 TOP-003-3
Requirement R4	TOP-003-3
Requirement R5	IRO-002-4 TOP-001-3
Requirement R6	TOP-003-3
Requirement R7	IRO-002-4 TOP-001-3

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-001-3
Requirement R2	IRO-009-1 TOP-001-3
Requirement R3	EOP-003-2, Requirement 1 (adoption held in abeyance in BC due to PA/PC dependencies) IRO-009-1
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 BC due to PA/PC dependencies) TOP-001-3
Requirements R2 and R3	TOP-001-3
Requirement R4	TOP-001-3 TOP-002-4 TOP-003-3

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

Updated by Order R-33-18

Introduction:

This document is to be used in conjunction with the NERC Glossary dated October 6, 2017.

- The NERC Glossary terms listed in Table 1 below are effective in BC on the date specified in the "Effective Date" column.
- Table 2 below outlines the adoption history by the BCUC of the NERC Glossaries in BC.
- Any NERC Glossary terms and definitions in the NERC Glossary that are not approved by FERC on or before November 30, 2017 are of no force or effect in BC.
- Any NERC Glossary terms that have been remanded or retired by NERC are of no force or effect in BC, with the exception of those remanded or retired NERC Glossary terms which have not yet been retired in BC.
- 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 BC.

Table 1 BC Effective Date Exceptions to Definitions in the October 6, 2017 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
BES Cyber Asset[2]	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] where this term is referenced
BES Cyber Asset	BCA	Report No. 10	R-39-17	Adoption	October 1, 2018

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

[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.

[3] CIP Version 5 standards include 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.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
BES Cyber System	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] 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[3] 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 Report	R-27-18A	Adoption	July 1, 2019
Cascading	-	Report No. 10	R-39-17	Adoption	October 1, 2017
CIP Exceptional Circumstance	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] where this term is referenced
CIP Senior Manager	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] 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 Report	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

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Control Center	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] where this term is referenced
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[3] where this term is referenced
Cyber Security Incident	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] where this term is referenced
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[3] 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
Electronic Access Control or Monitoring Systems	EACMS	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] 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[3] 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[3] where this term is referenced
Element	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Energy Emergency	-	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[3] 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[4]
Interactive Remote Access	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] where this term is referenced
Interchange Authority	IA	Report No. 10	R-39-17	Adoption	October 1, 2017
Interchange Meter Error (I_{ME})	-	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
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[3] 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

[4] The NERC Glossary term is associated with reliability standard that is dependent on the Planning Authority/Planning Coordinator function. The BCUC reasons for decision appended to Order R-41-13 (page 20), indicated that a separate process would be established to consider this matter as it pertains to BC.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Long-Term Transmission Planning Horizon	-	TPL-001-4 Report	R-27-18A	Adoption	July 1, 2019
Low Impact BES Cyber System Electronic Access Point[5]	LEAP	Report No. 10		Adoption	Not recommended for adoption in BC at this time
Low Impact External Routable Connectivity[5]	LERC	Report No. 10		Adoption	Not recommended for adoption in BC at this time
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
Operational Planning Analysis	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Operations Support Personnel	-	Report No. 8	R-38-15	Adoption	Align with effective date of Requirement R5 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[3] 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[3] where this term is referenced
Planning Assessment	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019

[5] Intended for CIP-003-6 and to be held in abeyance and be of no force or effect in BC due to technical suitability issues. When adopted by FERC, the NERC approved CIP-003-7(i) will retire the NERC Glossary terms. CIP-003-7(i) is anticipated to be assessed in the next MRS Assessment Report.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
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[3] where this term is referenced
Protected Cyber Assets	PCA	Report No. 10	R-39-17	Adoption	October 1, 2018
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 Maintenance Program	PSMP	Report No. 8	R-38-15	Adoption	Align with effective date of Requirement R1 of the PRC-005-2 standard where this term is referenced
Protection System Maintenance Program *(PRC-005-4)*[6]	PSMP	Report No. 9		-	Not recommended for adoption in BC at this time
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
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	-	Report No. 9	R-32-16A	Adoption	October 1, 2016

[6] Intended for reliability standard PRC-005-4 which was deferred by FERC and was not included in Assessment Report No. 9.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
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
Remedial Action Scheme	RAS	Report No. 1	G-67-09	Adoption	June 4, 2009
Remedial Action Scheme	RAS	Report No. 9		-	To be determined[4]
Removable Media	-	Report No. 10	R-39-17	Adoption	October 1, 2018
Reporting ACE	-	Report No. 11	R-33-18	Adoption	October 1, 2019
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[3] where this term is referenced
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

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Source Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Special Protection System (Remedial Action Scheme)	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 dependancies
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
System Operator	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards[3] 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	-	Report No. 10	R-39-17	Adoption	October 1, 2018
Transmission Customer	-	Report No. 10	R-39-17	Adoption	October 1, 2017
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[4]
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 BC

NERC Glossary of Terms Version Date	Assessment Report Number	BCUC Order Adoption Date	BCUC Order Adopting	Notes Pertaining to NERC Glossary Effective Dates
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 BC. 4. Any NERC Glossary terms that have been remanded or retired by NERC are of no force or effect in BC, with the exception of those remanded or retired NERC Glossary terms which have not yet been retired in BC. 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 BC.
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[3]	TPL-001-4	June 28, 2018	R-27-18A	
October 6, 2017	Report No. 11	October 1, 2018	R-33-18	

[1] The BAL-001-2 Glossary Terms (Interconnection, Regulation Reserve Sharing Group, Reporting Ace and Reserve Sharing Group Reporting Ace) became effective as of July 1, 2016.

[2] With the adoption of the NERC Glossary as part of MRS Assessment Report No. 9, the BAL-001-2 Glossary Terms were no longer exceptions to the NERC Glossary and so are not included in Table 1.

[3] Additional Glossary Terms pertaining to TPL-001-4 adopted by BCUC Order R-27-18A.

British Columbia Utilities Commission (BCUC)
Implementation Plan for Reliability Standards IRO-002-5 and TOP-001-4

Applicable Standard(s)

- IRO-002-5 - Reliability Coordination - Monitoring and Analysis
- TOP-001-4 - Transmission Operations

Requested Retirement(s)

- IRO-002-4 - Reliability Coordination - Monitoring and Analysis
- TOP-001-3 - Transmission Operations

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Reliability Coordinator
- Balancing Authority
- Transmission Operator
- Generator Operator
- Distribution Provider

General Considerations

The three-month implementation period for IRO-002-5 provides Reliability Coordinators with time to establish and document data exchange capabilities that are redundant and diversely routed, and to implement testing processes and procedures for redundant functionality. The proposed implementation plan presumes that IRO-002-4 is effective, or will become effective, on or before the effective date of IRO-002-5.

The implementation period for TOP-001-4 provides Transmission Operators (TOP) with time to revise and distribute data specifications required by TOP-003-3 Requirement R1 to include non-Bulk Electric System (BES) data identified by the TOP, and receive data from entities responsible for providing the data as required by TOP-003-3 Requirement R5. The implementation period also provides TOPs and Balancing Authorities (BAs) with time to establish and document data exchange capabilities that are redundant and diversely routed, and to implement testing processes and procedures for redundant functionality.

Effective Date

IRO-002-5

The standard shall become effective on January 1, 2019 after the BCUC's order approving the standard.

TOP-001-4

The standard shall become effective on October 1, 2020 (coincident with the effective date of the TOP-001-3 standard in British Columbia) after the BCUC's order approving the standard.

Retirement Date

IRO-002-4

Reliability Standard IRO-002-4 shall be retired immediately prior to the effective date of IRO-002-5 in the particular jurisdiction in which the revised standard is becoming effective.

TOP-001-3

Reliability Standard TOP-001-3 shall be retired immediately on the effective date of TOP-001-4.

Initial Performance of Periodic Requirements

IRO-002-5

The initial test of primary Control Center data exchange capabilities specified in Requirement R3 must be completed within 90 calendar days of the effective date of IRO-002-5.

TOP-001-4

The initial test of primary Control Center data exchange capabilities specified in Requirements R21 and R24 must be completed within 90 calendar days of the effective date of TOP-001-4.

British Columbia Utilities Commission (BCUC)
Implementation Plan for PRC-012-2 – Remedial Action Schemes (RAS)

Requested Approval

- PRC-012-2 – Remedial Action Schemes

Requested Retirements

- PRC-015-1 – Remedial Action Scheme Data and Documentation
- PRC-016-1 – Remedial Action Scheme Misoperations

Applicable Entities

- Reliability Coordinator
- RAS-entity – the Transmission Owner, Generator Owner or Distribution Provider that owns all or part of a RAS

General Considerations

Reliability Standard PRC-012-2 consolidates previously unapproved standards and revises other RAS-related standards. Reliability Standard PRC-012-2 also provides clear and unambiguous responsibilities to the specific users, owners and operators of the Bulk Electric System. Reliability Standard PRC-012-2 establishes a new working framework between RAS-entities, Planning Coordinators (PCs), and Reliability Coordinators (RCs), and this new framework will involve considerable start-up effort. As such, implementation of Reliability Standard PRC-012-2 will occur over a 36-month period after approval of the standard by the BCUC.

Limited Impact RAS

A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional review process of the Western Electricity Coordinating Council (WECC) and is classified as a Local Area Protection Scheme (LAPS) in WECC is recognized as a limited impact RAS upon the effective date of PRC-012-2 and is subject to all applicable requirements.

Effective Date

Reliability Standard PRC-012-2 shall become effective on October 1, 2021 after the BCUC's order approving the standard. Provisions concerning the initial performance of obligations under Requirements R1, R2, R4, R8 and R9 are outlined below.

Requirements R1, R2 and R4

Attachment 1, Section II Parts 6d) and 6e) as referenced from Requirement R1, Attachment 2 Section I Parts 7d) and 7e) as referenced from Requirement R2, and all of Requirement R4 are held in abeyance in British Columbia pending resolution of the Planning Authority/Planning Coordination role and responsibility process as managed by the BCUC. Pending the aforementioned process, these requirements shall be formally re-assessed in British Columbia to determine the effective date of the aforementioned attachment sections.

Requirement R8

For each RAS not designated as limited impact, initial performance of obligations under Requirement R8 must be completed at least once within six full calendar years after the effective date for PRC-012-2, as described above.

For each RAS designated as limited impact, initial performance of obligations under Requirement R8 must be completed at least once within twelve full calendar years after the effective date for PRC-012-2, as described above.

Requirement R9

For each Reliability Coordinator that does not have a RAS database, the initial obligation under Requirement R9 is to establish a database by the effective date of PRC-012-2.

Each Reliability Coordinator will perform the obligation of Requirement R9 within twelve full calendar months after the effective date of PRC-012-2, as described above.

Retirement of Existing Standards

The Reliability Standards for retirement shall be retired immediately prior to the effective date of PRC-012-2.

A. Introduction

1. **Title:** Balancing Authority Control

2. **Number:** BAL-005-1

3. **Purpose:** This standard establishes requirements for acquiring data necessary to calculate Reporting Area Control Error (Reporting ACE). The standard also specifies a minimum periodicity, accuracy, and availability requirement for acquisition of the data and for providing the information to the System Operator.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

Effective Date*: See Implementation Plan for BAL-005-1

B. Requirements and Measures

R1. The Balancing Authority shall use a design scan rate of no more than six seconds in acquiring data necessary to calculate Reporting ACE. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M1. Each Balancing Authority will have dated documentation demonstrating that the data necessary to calculate Reporting ACE was designed to be scanned at a rate of no more than six seconds. Acceptable evidence may include historical data, dated archive files; or data from other databases, spreadsheets, or displays that demonstrate compliance.

R2. A Balancing Authority that is unable to calculate Reporting ACE for more than 30-consecutive minutes shall notify its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M2. Each Balancing Authority will have dated records to show when it was unable to calculate Reporting ACE for more than 30 consecutive minutes and that it notified its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE. Such evidence may include, but is not limited to, dated voice recordings, operating logs, or other communication documentation.

R3. Each Balancing Authority shall use frequency metering equipment for the calculation of Reporting ACE: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

3.1. that is available a minimum of 99.95% for each calendar year; and,

3.2. with a minimum accuracy of 0.001 Hz.

M3. The Balancing Authority shall have evidence such as dated documents or other evidence in hard copy or electronic format showing the frequency metering equipment used for the calculation of Reporting ACE had a minimum availability of 99.95% for each calendar year and had a minimum accuracy of 0.001 Hz to demonstrate compliance with Requirement R3.

R4. The Balancing Authority shall make available to the operator information associated with Reporting ACE including, but not limited to, quality flags indicating missing or invalid data. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. Each Balancing Authority Area shall have evidence such as a graphical display or dated alarm log that provides indication of data validity for the real-time Reporting ACE based on both the calculated result and all of the associated inputs therein.

R5. Each Balancing Authority's system used to calculate Reporting ACE shall be available a minimum of 99.5% of each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M5. Each Balancing Authority will have dated documentation demonstrating that the system necessary to calculate Reporting ACE has a minimum availability of 99.5% for each calendar year. Acceptable evidence may include historical data, dated archive files; or data from other databases, spreadsheets, or displays that demonstrate compliance.

R6. Each Balancing Authority that is within a multiple Balancing Authority Interconnection shall implement an Operating Process to identify and mitigate errors affecting the accuracy of scan rate data used in the calculation of Reporting ACE for each Balancing Authority Area. *[Violation Risk Factor: Medium] [Time Horizon: Same-day Operations]*

M6. Each Balancing Authority shall have a current Operating Process meeting the provisions of Requirement R6 and evidence to show that the process was implemented, such as dated communications or incorporation in System Operator task verification.

R7. Each Balancing Authority shall ensure that each Tie-Line, Pseudo-Tie, and Dynamic Schedule with an Adjacent Balancing Authority is equipped with: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **7.1.** a common source to provide information to both Balancing Authorities for the scan rate values used in the calculation of Reporting ACE; and,
- **7.2.** a time synchronized common source to determine hourly megawatt-hour values agreed-upon to aid in the identification and mitigation of errors.

M7. The Balancing Authority shall have dated evidence such as voice recordings or transcripts, operator logs, electronic communications, or other equivalent evidence that will be used to demonstrate a common source for the components used in the calculation of Reporting ACE with its Adjacent Balancing Authority.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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 applicable entity shall keep data or evidence to show compliance for the current year, plus three previous calendar years.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Real-time Operations	Medium	N/A	N/A	N/A	Balancing Authority was using a design scan rate of greater than six seconds to acquire the data necessary to calculate Reporting ACE.
R2.	Real-time Operations	Medium	The Balancing Authority failed to notify its Reliability Coordinator within 45 minutes of the beginning of the inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 50 minutes from the beginning of the inability to calculate	The Balancing Authority failed to notify its Reliability Coordinator within 50 minutes of the beginning of an inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 55 minutes from the beginning of an inability to calculate	The Balancing Authority failed to notify its Reliability Coordinator within 55 minutes of the beginning of an inability to calculate Reporting ACE but notified its Reliability Coordinator in less than or equal to 60 minutes from the beginning of an inability to calculate	The Balancing Authority failed to notify its Reliability Coordinator within 60 minutes of the beginning of an inability to calculate Reporting ACE.

			Reporting ACE.	Reporting ACE.	Reporting ACE.	
R3.	Real-time Operations	Medium	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.95% of the calendar year but was available greater than or equal to 99.94 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.94% of the calendar year but was available greater than or equal to 99.93 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.93% of the calendar year but was available greater than or equal to 99.92 % of the calendar year.	The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE was available less than 99.92% of the calendar year Or The Balancing Authority's frequency metering equipment used for the calculation of Reporting ACE failed to have a minimum accuracy of 0.001 Hz.
R4.	Real-time Operations	Medium	N/A	N/A	N/A	The Balancing Authority failed to make available information indicating missing or invalid data associated with Reporting ACE to its operators.

R5.	Operations Assessment	Medium	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.5% of the calendar year but was available greater than or equal to 99.4 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.4% of the calendar year but was available greater than or equal to 99.3 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.3% of the calendar year but was available greater than or equal to 99.2 % of the calendar year.	The Balancing Authority's system used for the calculation of Reporting ACE was available less than 99.2% of the calendar year.
R6.	Same-day Operations	Medium	N/A	N/A	N/A	The Balancing Authority failed to implement an Operating Process to identify and mitigate errors affecting the scan-rate accuracy of data used in the calculation of Reporting ACE.
R7.	Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority failed to use a common source for Tie-Lines, Pseudo-ties and Dynamic Schedules with its Adjacent Balancing

						Authorities **Or** **The Balancing Authority failed to use a time synchronized common source for hourly megawatt hour values that are agreed-upon to aid in the identification and mitigation of errors.**

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	February 7,	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the	

	2013	Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
0.2b	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02) effective January 21, 2014.	
1	February 11, 2016	Adopted by NERC Board of Trustees	Complete re-write of standard
1	September 20. 2017	FERC Order No. 836 approved BAL-005-1.	

Rationale

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

Rationale for Requirement R1: Real-time operation of a Balancing Authority requires real-time information. A sufficient scan rate is key to an Operator's trust in real-time information. Without a sufficient scan rate, an operator may question the accuracy of data during events, which would degrade the operator's ability to maintain reliability.

Rationale for Requirement R2: The RC is responsible for coordinating the reliability of bulk electric systems for member BA's. When a BA is unable to calculate its ACE for an extended period of time, this information must be communicated to the RC within 15 minutes thereafter so that the RC has sufficient knowledge of system conditions to assess any unintended reliability consequences that may occur on the wide area.

Rationale for Requirement R3: Frequency is the basic measurement for interconnection health, and a critical component for calculating Reporting ACE. Without sufficient available frequency data the BA operator will lack situational awareness and will be unable to make correct decisions when maintaining reliability.

Rationale for Requirement R4: System operators utilize Reporting ACE as a primary metric to determine operating actions or instructions. When data inputs into the ACE calculation are incorrect, the operator should be made aware through visual display. When an operator questions the validity of data, actions are delayed and the probability of adverse events occurring can increase.

Rationale for Requirement R5: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Since Reporting ACE is a measure of the BA's reliability performance for BAL-001, and BAL-002, it is critical that Reporting ACE be sufficiently available to assure reliability.

Rationale for Requirement R6: Reporting ACE is a measure of the BA's reliability performance for BAL-001, and BAL-002. Without a process to address persistent errors in the ACE calculation, the operator can lose trust in the validity of Reporting ACE resulting in delayed or incorrect decisions regarding the reliability of the bulk electric system.

Rationale for Requirement R7: Reporting ACE is an essential measurement of the BA's contribution to the reliability of the Interconnection. Common source data is critical to calculating Reporting ACE that is consistent between Balancing Authorities. When data sources are not common, confusion can be created between BAs resulting in delayed or incorrect operator action.

Supplemental Material

The intent of Requirement R7 Part 7.1 is to provide accuracy in the measurement and calculations used in Reporting ACE. It specifies the need for common metering points for instantaneous values for the tie-line megawatt flow values between Balancing Authority Areas. Common data source requirements also apply to instantaneous values for pseudo-ties and dynamic schedules, and can extend to more than two Balancing Authorities that participate in allocating shares of a generation resource in supplementary regulation, for example.

The intent of Requirement R7 Part 7.2 is to enable accuracy in the measurements and calculations used in Reporting ACE. It specifies the need for common metering points for hourly accumulated values for the time synchronized tie line MWh values agreed-upon between Balancing Authority Areas. These time synchronized agreed-upon values are necessary for use in the Operating Process required in R6 to identify and mitigate errors in the scan-rate values used in Reporting ACE.

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5.1a

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1a:

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.

5. Effective Dates*: See footnote page 1.

1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

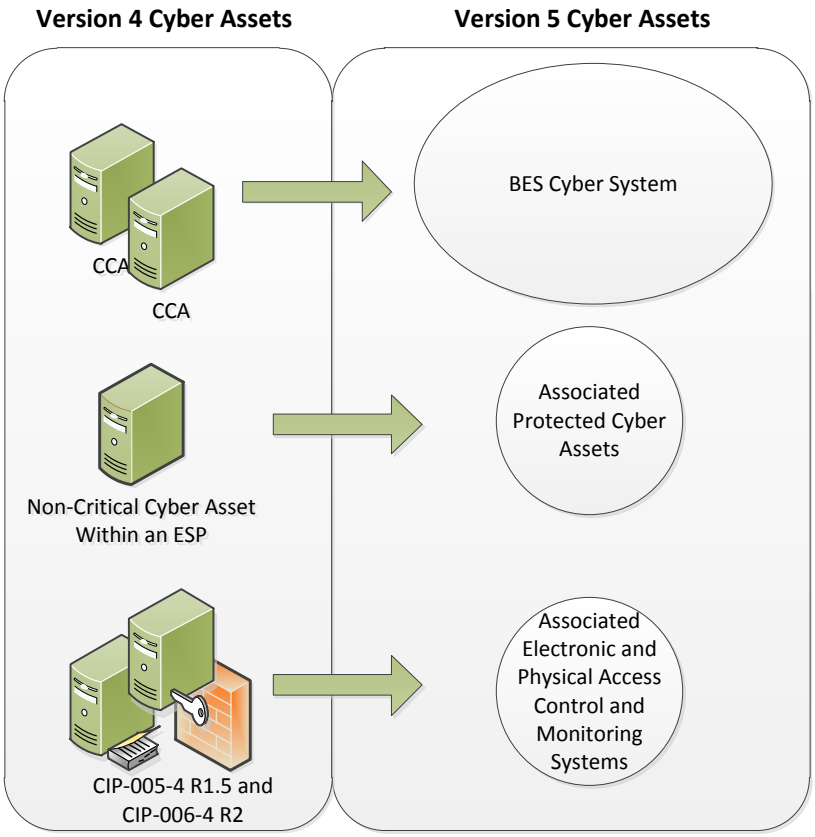
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation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

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

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

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

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

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

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

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

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

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

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

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

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

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

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

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

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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 Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

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

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower	Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower	Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5.1a - Attachment 1

Impact Rating Criteria

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

1. High Impact Rating (H)

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

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

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

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

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

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

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

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

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

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

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

3. Low Impact Rating (L)

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

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

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

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

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

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

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

Balancing Load and Generation

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

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

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

Controlling Frequency (Real Power)

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

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

Controlling Voltage (Reactive Power)

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

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

Managing Constraints

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

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

Monitoring and Control

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

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

Restoration of BES

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

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

Situational Awareness

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

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

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

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

Applicability to Distribution Providers

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

Requirement R1:

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

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

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

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

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

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

Medium Impact Rating (M)

Generation

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

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

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

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

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

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

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

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

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

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

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

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

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

    - Excluded radial facilities that would only provide support for single generation facilities.

    - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

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

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

    - 230 kV –> 700 MVA

    - 345 kV –> 1,300 MVA

    - 500 kV –> 2,000 MVA

    - 765 kV –> 3,000 MVA

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

    - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

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

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

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

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

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

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

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

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

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

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

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

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

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

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

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

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

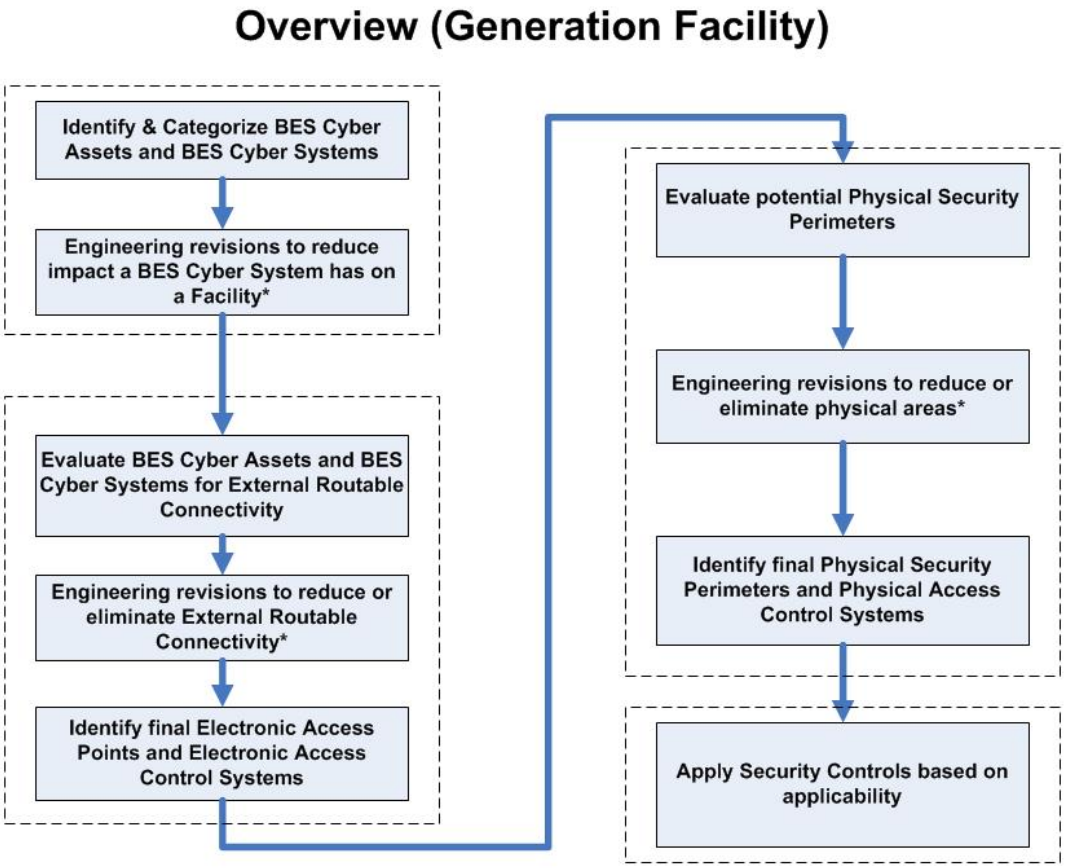
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific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

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

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

Use Case: CIP Process Flow

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



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

Rationale:

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

Rationale for R1:

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

Rationale for R2:

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

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.	Update

		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.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	

Appendix 1

Requirement Number and Text of Requirement
CIP-002-5.1, Requirement R1 R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). Attachment 1, Criterion 2.1 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following: 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
Questions
Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1

regarding the use of the phrase "shared BES Cyber Systems."

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

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

Responses

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

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

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

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

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

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

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

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

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

The phrase applies to each discrete BES Cyber System.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

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

4.1.1 Balancing Authority

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

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

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

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

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-5:

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.

5. Effective Dates*: See footnote page 1.

6. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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 provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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

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

B. Requirements and Measures

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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 Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

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

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 18 calendar months of the previous approval.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented	did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 17 calendar months but did complete this approval	complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	in less than or equal to 18 calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the change. (R3)		Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

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

Rationale for R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-003-5 Requirements R1 and R2 eliminated redundant language in VSLs.

A. Introduction

1. **Title:** **Facility Interconnection Requirements**

2. **Number:** FAC-001-3

3. **Purpose:** To avoid adverse impacts on the reliability of the Bulk Electric System, Transmission Owners and applicable Generator Owners must document and make Facility interconnection requirements available so that entities seeking to interconnect will have the necessary information.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Transmission Owner

   4.1.2 Applicable Generator Owner

   4.1.2.1 Generator Owner with a fully executed Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.

5. **Effective Date*:** See Implementation Plan for FAC-001-3.

B. Requirements and Measures

R1. Each Transmission Owner shall document Facility interconnection requirements, update them as needed, and make them available upon request. Each Transmission Owner's Facility interconnection requirements shall address interconnection requirements for: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. generation Facilities;

1.2. transmission Facilities; and

1.3. end-user Facilities.

M1. Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R1.

R2. Each applicable Generator Owner shall document Facility interconnection requirements and make them available upon request within 45 calendar days of full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements) that it met all requirements in Requirement R2.

R3. Each Transmission Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*

3.1. Procedures for coordinated studies of new or materially modified existing interconnections and their impacts on affected system(s).

3.2. Procedures for notifying those responsible for the reliability of affected system(s) of new or materially modified existing interconnections.

3.3. Procedures for confirming with those responsible for the reliability of affected systems of new or materially modified transmission Facilities are within a Balancing Authority Area's metered boundaries.

M3. Each Transmission Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R3.

R4. Each applicable Generator Owner shall address the following items in its Facility interconnection requirements: *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*

4.1. Procedures for coordinated studies of new interconnections and their impacts on affected system(s).

4.2. Procedures for notifying those responsible for the reliability of affected system(s) of new interconnections.

4.3. Procedures for confirming with those responsible for the reliability of affected systems of new or materially modified generation Facilities are within a Balancing Authority Area's metered boundaries.

M4. Each applicable Generator Owner shall have evidence (such as dated, documented Facility interconnection requirements addressing the procedures) that it met all requirements in Requirement R4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

The responsible entities shall retain documentation as evidence for three years.

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Check

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Lower	N/A	The Transmission Owner documented Facility interconnection requirements and updated them as needed, but failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements and made them available upon request, but failed to update them as needed. OR The Transmission Owner documented Facility interconnection requirements, updated them as needed, and made them available upon request, but	The Transmission Owner documented Facility interconnection requirements, but failed to update them as needed and failed to make them available upon request. OR The Transmission Owner documented Facility interconnection requirements, updated them as needed, and made them available upon request, but failed to address interconnection requirements for two of the Facilities as specified in R1, Parts 1.1, 1.2, or 1.3.	The Transmission Owner did not document Facility interconnection requirements.

				failed to address interconnection requirements for one of the Facilities as specified in R1, Parts 1.1, 1.2, or 1.3.		
R2	Long-term Planning	Lower	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 45 calendar days but less than or equal to 60 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 60 calendar days but less than or equal to 70 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 70 calendar days but less than or equal to 80 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.	The applicable Generator Owner failed to document Facility interconnection requirements and make them available upon request until more than 80 calendar days after full execution of an Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission system.

R3	Long-term Planning	Lower	N/A	The Transmission Owner failed to address one part of Requirement R3 Part 3.1 through Part 3.3.	The Transmission Owner failed to address two parts of Requirement R3 Part 3.1 through Part 3.3.	The Transmission Owner failed to address Requirement R3 Part 3.1 through Part 3.3.
R4	Long-term Planning	Lower	N/A	The Generator Owner failed to address one part of Requirement R4 Part 4.1 through Part 4.3.	The Generator Owner failed to address two parts of Requirement R4 Part 4.1 through Part 4.3.	The Generator Owner failed to address Requirement R4 Part 4.1 through Part 4.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1		Added requirements for Generator Owner and brought overall standard format up to date.	Revision under Project 2010-07
1	February 9, 2012	Adopted by the Board of Trustees	
1	September 19, 2013	A FERC order was issued on September 19, 2013, approving FAC-001-1. This standard became enforceable on November 25, 2013 for Transmission Owners. For Generator Owners, the standard becomes enforceable on January 1, 2015.	
2		Revisions to implement the recommendations of the FAC Five-Year Review Team.	Revision under Project 2010-02
2	August 14, 2014	Adopted by the Board of Trustees	
2	November 6, 2014	FERC letter order issued approving FAC-001-2.	
3	February 11, 2016	Adopted by the Board of Trustees	Moved BAL-005-0.2b Requirement R1 into FAC-001-3 Requirements R3 and R4
3	September 20, 2017	FERC Order No. 836 issued approving FAC-001-3	

Supplemental Material

Guidelines and Technical Basis

Entities should have documentation to support the technical rationale for determining whether an existing interconnection was "materially modified." Recognizing that what constitutes a "material modification" will vary from entity to entity, the intent is for this determination to be based on engineering judgment.

Requirement R3:

Originally the Parts of R3, with the exception of the first two bullets, which were added by the Project 2010-02 drafting team, this list has been moved to the Guidelines and Technical Basis section to provide entities with the flexibility to determine the Facility interconnection requirements that are technically appropriate for their respective Facilities. Including them as Parts of R3 was deemed too prescriptive, as frequently some items in the list do not apply to all applicable entities – and some applicable entities will have requirements that are not included in this list.

Each Transmission Owner and applicable Generator Owner should consider the following items in the development of Facility interconnection requirements:

- Procedures for requesting a new Facility interconnection or material modification to an existing interconnection
- Data required to properly study the interconnection
- Voltage level and MW and MVAR capacity or demand at the point of interconnection
- Breaker duty and surge protection
- System protection and coordination
- Metering and telecommunications
- Grounding and safety issues
- Insulation and insulation coordination
- Voltage, Reactive Power (including specifications for minimum static and dynamic reactive power requirements), and power factor control
- Power quality impacts
- Equipment ratings
- Synchronizing of Facilities
- Maintenance coordination
- Operational issues (abnormal frequency and voltages)
- Inspection requirements for new or materially modified existing interconnections
- Communications and procedures during normal and emergency operating conditions

Supplemental Material

Rationale

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

Rationale for Requirement R3.3: Consistent with the Functional Model, there cannot be an assumption that the entity owning the transmission will be the same entity providing the BA function. It is the responsibility of the party interconnecting to make appropriate arrangements with a Balancing Authority to ensure its Facilities are within the BA's metered boundaries, which also serves to facilitate the process of the coordination between the two entities that will be required under numerous other standards upon the start of operation. Under 3.3, the Transmission Owner is responsible for confirming that the party interconnecting has made appropriate provisions with a Balancing Authority to operate within its metered boundaries.

Rationale for Requirement R4.3: Consistent with the Functional Model, there cannot be an assumption that the entity owning the generation will be the same entity providing the BA function. It is the responsibility of the party interconnecting to make appropriate arrangements with a Balancing Authority to ensure its Facilities are within the BA's metered boundaries, which also serves to facilitate the process of the coordination between the two entities that will be required under numerous other standards upon the start of operation. Under 4.3, the Generator Owner is responsible for confirming that the party interconnecting has made appropriate provisions with a Balancing Authority to operate within its metered boundaries.

A. Introduction

1. **Title:** **Reliability Coordination – Monitoring and Analysis**

2. **Number:** IRO-002-5

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. Each Reliability Coordinator shall have data exchange capabilities with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for it to perform its Operational Planning Analyses. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Each Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, a document that lists its data exchange capabilities with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for it to perform its Operational Planning Analyses.

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 R1, R2, and R4 and Measures M1, 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.	The Reliability Coordinator did not have data exchange capabilities for performing its Operational Planning Analyses with one applicable entity, or 5% or less of the applicable entities, whichever is greater.	The Reliability Coordinator did not have data exchange capabilities for performing its Operational Planning Analyses with two applicable entities, or more than 5% or less than or equal to 10% of the applicable entities, whichever is greater.	The Reliability Coordinator did not have data exchange capabilities for performing its Operational Planning Analyses with three applicable entities, or more than 10% or less than or equal to 15% of the applicable entities, whichever is greater.	The Reliability Coordinator did not have data exchange capabilities for performing its Operational Planning Analyses with four or more applicable entities or greater than 15% of the applicable entities, whichever is greater.
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	The Reliability Coordinator tested its primary Control Center data exchange	The Reliability Coordinator tested its primary Control Center data exchange	The Reliability Coordinator tested its primary Control Center data exchange

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	capabilities specified in Requirement R2 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 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.	capabilities specified in Requirement R2 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 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.	capabilities specified in Requirement R2 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 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.	capabilities specified in Requirement R2 for 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.
R4.	N/A	N/A	N/A	The Reliability Coordinator failed to provide its System Operator with the authority to approve planned outages and

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				redundant infrastructure.

D. Regional Variances

None.

E. Associated Documents

The Implementation Plan and other project documents can be found on the project page.

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	

Guidelines and Technical Basis

None

Rationale

During development of IRO-002-5, text boxes are embedded within the standard to explain the rationale for various parts of the standard. Upon Board adoption of IRO-002-5, the text from the rationale text boxes will be moved to this section.

Rationale text from the development of IRO-002-4 in Project 2014-03 follows. Additional information can be found on the Project 2014-03 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:
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):
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 Real-time Reliability Monitoring and Analysis Capabilities**

2. **Number:** **IRO-018-1(i)**

3. **Purpose:** Establish requirements for Real-time monitoring and analysis capabilities to support reliable System operations.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinators

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

B. Requirements and Measures

R1. Each Reliability Coordinator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

1.1. Criteria for evaluating the quality of Real-time data;

1.2. Provisions to indicate the quality of Real-time data to the System Operator; and

1.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.

M1. Each Reliability Coordinator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R1; and 2) evidence the Reliability Coordinator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator or supporting logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R2. Each Reliability Coordinator shall implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. Criteria for evaluating the quality of analysis used in its Real-time Assessments;

2.2. Provisions to indicate the quality of analysis used in its Real-time Assessments; and

2.3. Actions to address analysis quality issues affecting its Real-time Assessments.

M2. Each Reliability Coordinator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments as specified in Requirement R2. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R2; and 2) evidence the Reliability Coordinator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R3. Each Reliability Coordinator shall have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. Each Reliability Coordinator shall have evidence of an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. This evidence could include, but is not limited to, operator logs, computer printouts, system specifications, or other evidence.

C. Compliance

1. Compliance Monitoring Process

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

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

The Reliability Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Reliability Coordinator shall retain evidence of compliance for Requirements R1 and R3 and Measures M1 and M3 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Reliability Coordinator shall retain evidence of compliance for Requirement R2 and Measure M2 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

The Compliance Enforcement Authority 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 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 Reliability Coordinator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include one of the elements listed in Part 1.1 through Part 1.3.	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include two of the elements listed in Part 1.1 through Part 1.3.	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include any of the elements listed in Part 1.1 through Part 1.3; OR The Reliability Coordinator did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments.
R2.	N/A	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of	The Reliability Coordinator's Operating Process or Operating Procedure to address the quality of

		analysis used in its Real-time Assessments did not include one of the elements listed in Part 2.1 through Part 2.3.	analysis used in its Real-time Assessments did not include two of the elements listed in Part 2.1 through Part 2.3.	analysis used in its Real-time Assessments did not include any of the elements listed in Part 2.1 through Part 2.3; OR The Reliability Coordinator did not implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments.
R3.	N/A	N/A	The Reliability Coordinator has an alarm process monitor but the alarm process monitor did not provide a notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor occurred.	The Reliability Coordinator does not have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	October 30, 3015	New standard developed in Project 2009-02 to respond to recommendations in Real-time Best Practices Task Force Report and FERC directives.	N/A
1	May 5, 2016	Adopted by the Board of Trustees.	New
1	September 22, 2016	FERC Order issued approving IRO-018-1. Docket No. RD16-6-000	
1(i)	September 22, 2016	FERC directive to change Requirement 1 from 'medium' to 'high'. Docket No. RD16-6-000	Revised
1(i)	November 2, 2016	Adopted by the Board of Trustees	New
1(i)	December 14, 2016	FERC letter Order approving revisions to the VRFs for R1 from 'medium' to 'high'. Docket No. RD16-6-001.	

Guidelines and Technical Basis

Real-time monitoring, or *monitoring* the Bulk Electric System (BES) in Real-time, is a primary function of Reliability Coordinators (RCs), Transmission Operators (TOPs), and Balancing Authorities (BAs) as required by TOP and IRO Reliability Standards. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. Real-time monitoring may include the following activities performed in Real-time:

- Acquisition of operating data;
- Display of operating data as needed for visualization of system conditions;
- Audible or visual alerting when warranted by system conditions; and
- Audible or visual alerting when monitoring and analysis capabilities degrade or become unavailable.

Requirement R1

The RC uses a set of Real-time data identified in IRO-010-1a Requirement R1 and IRO-010-2 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Requirements to perform monitoring and Real-time Assessments appear in other Reliability Standards.

The RC's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed IRO-018-1 Requirement R1 Part 1.1. The criteria support identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 specifies the RC shall include actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments. Requirement R1 Part 1.3 is focused on addressing data point quality issues affecting Real-time Assessments. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R1 Part 1.3.

The RC's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the RC to meet its obligations for performing the Real-time Assessment. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the RC;

- Following processes established for resolving data conflicts as specified in IRO-010-1a, IRO-010-2, or other applicable Reliability Standards;
- Taking corrective actions on the RC's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the RC's Real-time Assessment; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the quality of the Real-time Assessment so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R2

Requirement R2 ensures RCs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

Examples of the types of criteria used to evaluate the quality of analysis used in Real-time Assessments may include solution tolerances, mismatches with Real-time data, convergences, etc.

The Operating Process or Operating Procedure must describe how the quality of analysis results used in Real-time Assessment will be shown to operating personnel.

Requirement R3

Requirement R3 addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

An alarm process monitor could be an application within a Real-time monitoring system or it could be a separate system. 'Heartbeat' or 'watchdog' monitors are examples of an alarm process monitor. An alarm process monitor should be designed and implemented such that a stall of the Real-time monitoring alarm processor does not cause a failure of the alarm process monitor.

Rationale

Rationale for Requirement R1: The Reliability Coordinator (RC) uses a set of Real-time data identified in IRO-010-1a Requirement R1 and IRO-010-2 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Requirements to perform Real-time monitoring and Real-time Assessments appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 of this standard specifies the RC shall include actions to address Real-time data quality issues affecting its Real-time Assessments in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process used to resolve data conflicts required by IRO-010-2 Requirement R3 Part 3.2 provided that this process addresses Real-time data quality issues.

The revision in Part 1.3 to address Real-time data quality issues *when data quality affects Real-time Assessments* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R2: Requirement R2 ensures RCs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

The Operating Process or Operating Procedure must include provisions for how the quality of analysis results used in Real-time Assessment will be shown to operating personnel. Operating personnel includes System Operators and staff responsible for supporting Real-time operations.

Rationale for Requirement R3: The requirement addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

The requirement in Draft Two of the proposed standard has been revised for clarity by removing the term *independent*. The alarm process monitor must be able to provide notification of failure of the Real-time monitoring alarm processor. This capability could be provided by an application within a Real-time monitoring system or by a separate component used by the System Operator. The alarm process monitor must not fail with a simultaneous failure of the Real-time monitoring alarm processor.

A. Introduction

1. **Title:** Remedial Action Schemes

2. **Number:** PRC-012-2

3. **Purpose:** To ensure that Remedial Action Schemes (RAS) do not introduce unintentional or unacceptable reliability risks to the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinator

   4.1.2. Planning Coordinator

   4.1.3. RAS-entity – the Transmission Owner, Generator Owner, or Distribution Provider that owns all or part of a RAS

   4.2. Facilities:

   4.2.1. Remedial Action Schemes (RAS)

5. **Effective Date*:** See the Implementation Plan for PRC-012-2.

B. Requirements and Measures

R1. Prior to placing a new or functionally modified RAS in service or retiring an existing RAS, each RAS-entity shall provide the information identified in Attachment 1 for review to the Reliability Coordinator(s) where the RAS is located. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Acceptable evidence may include, but is not limited to, a copy of the Attachment 1 documentation and the dated communications with the reviewing Reliability Coordinator(s) in accordance with Requirement R1.

R2. Each Reliability Coordinator that receives Attachment 1 information pursuant to Requirement R1 shall, within four full calendar months of receipt or on a mutually agreed upon schedule, perform a review of the RAS in accordance with Attachment 2, and provide written feedback to each RAS-entity. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Acceptable evidence may include, but is not limited to, dated reports, checklists, or other documentation detailing the RAS review, and the dated communications with the RAS-entity in accordance with Requirement R2.

R3. Prior to placing a new or functionally modified RAS in service or retiring an existing RAS, each RAS-entity that receives feedback from the reviewing Reliability Coordinator(s) identifying reliability issue(s) shall resolve each issue to obtain

approval of the RAS from each reviewing Reliability Coordinator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Acceptable evidence may include, but is not limited to, dated documentation and communications with the reviewing Reliability Coordinator that no reliability issues were identified during the review or that all identified reliability issues were resolved in accordance with Requirement R3.

R4. Each Planning Coordinator, at least once every five full calendar years, shall: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

4.1. Perform an evaluation of each RAS within its planning area to determine whether:

4.1.1. The RAS mitigates the System condition(s) or Contingency(ies) for which it was designed.

4.1.2. The RAS avoids adverse interactions with other RAS, and protection and control systems.

4.1.3. For limited impact[1] RAS, the inadvertent operation of the RAS or the failure of the RAS to operate does not cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

4.1.4. Except for limited impact RAS, the possible inadvertent operation of the RAS, resulting from any single RAS component malfunction satisfies all of the following:

4.1.4.1. The BES shall remain stable.

4.1.4.2. Cascading shall not occur.

4.1.4.3. Applicable Facility Ratings shall not be exceeded.

4.1.4.4. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.

4.1.4.5. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.

4.1.5. Except for limited impact RAS, a single component failure in the RAS, when the RAS is intended to operate does not prevent the BES from meeting the same performance requirements (defined in Reliability

[1] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed.

4.2. Provide the results of the RAS evaluation including any identified deficiencies to each reviewing Reliability Coordinator and RAS-entity, and each impacted Transmission Planner and Planning Coordinator.

M4. Acceptable evidence may include, but is not limited to, dated reports or other documentation of the analyses comprising the evaluation(s) of each RAS and dated communications with the RAS-entity(ies), Transmission Planner(s), Planning Coordinator(s), and the reviewing Reliability Coordinator(s) in accordance with Requirement R4.

R5. Each RAS-entity, within 120 full calendar days of a RAS operation or a failure of its RAS to operate when expected, or on a mutually agreed upon schedule with its reviewing Reliability Coordinator(s), shall: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. Participate in analyzing the RAS operational performance to determine whether:

5.1.1. The System events and/or conditions appropriately triggered the RAS.

5.1.2. The RAS responded as designed.

5.1.3. The RAS was effective in mitigating BES performance issues it was designed to address.

5.1.4. The RAS operation resulted in any unintended or adverse BES response.

5.2. Provide the results of RAS operational performance analysis that identified any deficiencies to its reviewing Reliability Coordinator(s).

M5. Acceptable evidence may include, but is not limited to, dated documentation detailing the results of the RAS operational performance analysis and dated communications with participating RAS-entities and the reviewing Reliability Coordinator(s) in accordance with Requirement R5.

R6. Each RAS-entity shall participate in developing a Corrective Action Plan (CAP) and submit the CAP to its reviewing Reliability Coordinator(s) within six full calendar months of: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Long-term Planning]*

- Being notified of a deficiency in its RAS pursuant to Requirement R4, or
- Notifying the Reliability Coordinator of a deficiency pursuant to Requirement R5, Part 5.2, or
- Identifying a deficiency in its RAS pursuant to Requirement R8.

M6. Acceptable evidence may include, but is not limited to, a dated CAP and dated communications among each reviewing Reliability Coordinator and each RAS-entity in accordance with Requirement R6.

R7. Each RAS-entity shall, for each of its CAPs developed pursuant to Requirement R6: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Long-term Planning]*

7.1. Implement the CAP.

7.2. Update the CAP if actions or timetables change.

7.3. Notify each reviewing Reliability Coordinator if CAP actions or timetables change and when the CAP is completed.

M7. Acceptable evidence may include, but is not limited to, dated documentation such as CAPs, project or work management program records, settings sheets, work orders, maintenance records, and communication with the reviewing Reliability Coordinator(s) that documents the implementation, updating, or completion of a CAP in accordance with Requirement R7.

R8. Each RAS-entity shall participate in performing a functional test of each of its RAS to verify the overall RAS performance and the proper operation of non-Protection System components: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

- At least once every six full calendar years for all RAS not designated as limited impact, or
- At least once every twelve full calendar years for all RAS designated as limited impact

M8. Acceptable evidence may include, but is not limited to, dated documentation detailing the RAS operational performance analysis for a correct RAS segment or an end-to-end operation (Measure M5 documentation), or dated documentation demonstrating that a functional test of each RAS segment or an end-to-end test was performed in accordance with Requirement R8.

R9. Each Reliability Coordinator shall update a RAS database containing, at a minimum, the information in Attachment 3 at least once every twelve full calendar months. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M9. Acceptable evidence may include, but is not limited to, dated spreadsheets, database reports, or other documentation demonstrating a RAS database was updated in accordance with Requirement R9.

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 RAS-entity (Transmission Owner, Generator Owner, and Distribution Provider) shall each keep data or evidence to show compliance with Requirements R1, R3, R5, R6, R7, and R8, and Measures M1, M3, M5, M6, M7, and M8 since the last audit, 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 each keep data or evidence to show compliance with Requirements R2 and R9, and Measures M2 and M9 since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Planning Coordinator shall each keep data or evidence to show compliance with Requirement R4 and Measure M4 since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a RAS-entity (Transmission Owner, Generator Owner or Distribution Provider), Reliability Coordinator, or Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until mitigation is completed and approved, or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and 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 RAS-entity failed to provide the information identified in Attachment 1 to each Reliability Coordinator prior to placing a new or functionally modified RAS in service or retiring an existing RAS in accordance with Requirement R1.
R2.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by less than or equal to 30 full calendar days.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by more than 30 full calendar days but less than or equal to 60 full calendar days.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by more than 60 full calendar days but less than or equal to 90 full calendar days.	The reviewing Reliability Coordinator performed the review and provided the written feedback in accordance with Requirement R2, but was late by more than 90 full calendar days. OR The reviewing Reliability Coordinator failed to perform the review or provide feedback in accordance with Requirement R2.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	N/A	N/A	N/A	The RAS-entity failed to resolve identified reliability issue(s) to obtain approval from each reviewing Reliability Coordinator prior to placing a new or functionally modified RAS in service or retiring an existing RAS in accordance with Requirement R3.
R4.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by less than or equal to 30 full calendar days.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by more than 30 full calendar days but less than or equal to 60 full calendar days.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by more than 60 full calendar days but less than or equal to 90 full calendar days. OR The Planning Coordinator performed the evaluation in accordance with Requirement R4, but failed to evaluate one of the Parts 4.1.1 through 4.1.5.	The Planning Coordinator performed the evaluation in accordance with Requirement R4, but was late by more than 90 full calendar days. OR The Planning Coordinator performed the evaluation in accordance with Requirement R4, but failed to evaluate two or more of the Parts 4.1.1 through 4.1.5. OR The Planning Coordinator

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				performed the evaluation in accordance with Requirement R4, but failed to provide the results to one or more of the receiving entities listed in Part 4.2. OR The Planning Coordinator failed to perform the evaluation in accordance with Requirement R4.
R5.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by less than or equal to 10 full calendar days.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by more than 10 full calendar days but less than or equal to 20 full calendar days.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by more than 20 full calendar days but less than or equal to 30 full calendar days. OR The RAS-entity performed the analysis in accordance with Requirement R5, but failed to address one of the Parts 5.1.1 through 5.1.4.	The RAS-entity performed the analysis in accordance with Requirement R5, but was late by more than 30 full calendar days. OR The RAS-entity performed the analysis in accordance with Requirement R5, but failed to address two or more of the Parts 5.1.1 through 5.1.4. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The RAS-entity performed the analysis in accordance with Requirement R5, but failed to provide the results (Part 5.2) to one or more of the reviewing Reliability Coordinator(s). OR The RAS-entity failed to perform the analysis in accordance with Requirement R5.
R6.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by less than or equal to 10 full calendar days.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by more than 10 full calendar days but less than or equal to 20 full calendar days.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by more than 20 full calendar days but less than or equal to 30 full calendar days.	The RAS-entity developed a Corrective Action Plan and submitted it to its reviewing Reliability Coordinator(s) in accordance with Requirement R6, but was late by more than 30 full calendar days. OR The RAS-entity developed a Corrective Action Plan but failed to submit it to one or more of its reviewing

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Reliability Coordinator(s) in accordance with Requirement R6. OR The RAS-entity failed to develop a Corrective Action Plan in accordance with Requirement R6.
R7.	The RAS-entity implemented a CAP in accordance with Requirement R7, Part 7.1, but failed to update the CAP (Part 7.2) if actions or timetables changed, or failed to notify (Part 7.3) each of the reviewing Reliability Coordinator(s) of the updated CAP or completion of the CAP.	N/A	N/A	The RAS-entity failed to implement a CAP in accordance with Requirement R7, Part 7.1.
R8.	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by less than or equal to 30 full calendar days.	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by more than 30 full calendar days but less than or equal to 60	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by more than 60 full calendar days but less than or equal to 90	The RAS-entity performed the functional test for a RAS as specified in Requirement R8, but was late by more than 90 full calendar days.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		full calendar days.	full calendar days.	OR The RAS-entity failed to perform the functional test for a RAS as specified in Requirement R8.
R9.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9, but was late by less than or equal to 30 full calendar days.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9, but was late by more than 30 full calendar days but less than or equal to 60 full calendar days.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9, but was late by more than 60 full calendar days but less than or equal to 90 full calendar days.	The Reliability Coordinator updated the RAS database in accordance with Requirement R9 but was late by more than 90 full calendar days. OR The Reliability Coordinator failed to update the RAS database in accordance with Requirement R9.

D. Regional Variances

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by the Board of Trustees	
0	March 16, 2007	Identified by Commission as “fill-in-the-blank” with no action taken on the standard	
1	November 13, 2014	Adopted by the Board of Trustees	
1	November 19, 2015	Accepted by Commission for informational purposes only	
2	May 5, 2016	Adopted by Board of Trustees	
2	September 20, 2017	FERC Order No. 837 issued approving PRC-012-2	

Attachment 1
Supporting Documentation for RAS Review

The following checklist identifies important Remedial Action Scheme (RAS) information for each new or functionally modified[2] RAS that the RAS-entity must document and provide to the reviewing Reliability Coordinator(s) (RC). If an item on this list does not apply to a specific RAS, a response of "Not Applicable" for that item is appropriate. When RAS are submitted for functional modification review and approval, only the proposed modifications to that RAS require review; however, the RAS-entity must provide a summary of the existing functionality. The RC may request additional information on any aspect of the RAS as well as any reliability issue related to the RAS. Additional entities (without decision authority) may be part of the RAS review process at the request of the RC.

I. General

1. Information such as maps, one-line drawings, substation and schematic drawings that identify the physical and electrical location of the RAS and related facilities.
2. Functionality of new RAS or proposed functional modifications to existing RAS and documentation of the pre- and post-modified functionality of the RAS.
3. The Corrective Action Plan (CAP) if RAS modifications are proposed in a CAP.
4. Data to populate the RAS database:
    a. RAS name.
    b. Each RAS-entity and contact information.
    c. Expected or actual in-service date; most recent RC-approval date (Requirement R3); most recent evaluation date (Requirement R4); and date of retirement, if applicable.
    d. System performance issue or reason for installing the RAS (e.g., thermal overload, angular instability, poor oscillation damping, voltage instability, under- or over-voltage, or slow voltage recovery).
    e. Description of the Contingencies or System conditions for which the RAS was designed (i.e., initiating conditions).
    f. Action(s) to be taken by the RAS.
    g. Identification of limited impact[3] RAS.
    h. Any additional explanation relevant to high-level understanding of the RAS.

---

[2] Functionally modified: Any modification to a RAS consisting of any of the following:
- Changes to System conditions or contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

[3] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

II. Functional Description and Transmission Planning Information

1. Contingencies and System conditions that the RAS is intended to remedy.
2. The action(s) to be taken by the RAS in response to disturbance conditions.
3. A summary of technical studies, if applicable, demonstrating that the proposed RAS actions satisfy System performance objectives for the scope of System events and conditions that the RAS is intended to remedy. The technical studies summary shall also include information such as the study year(s), System conditions, and Contingencies analyzed on which the RAS design is based, and the date those technical studies were performed.
4. Information regarding any future System plans that will impact the RAS.
5. RAS-entity proposal and justification for limited impact designation, if applicable.
6. Documentation describing the System performance resulting from the possible inadvertent operation of the RAS, except for limited impact RAS, caused by any single RAS component malfunction. Single component malfunctions in a RAS not determined to be limited impact must satisfy all of the following:
    a. The BES shall remain stable.
    b. Cascading shall not occur.
    c. Applicable Facility Ratings shall not be exceeded.
    d. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.
    e. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.
7. An evaluation indicating that the RAS settings and operation avoid adverse interactions with other RAS, and protection and control systems.
8. Identification of other affected RCs.

III. Implementation

1. Documentation describing the applicable equipment used for detection, dc supply, communications, transfer trip, logic processing, control actions, and monitoring.
2. Information on detection logic and settings/parameters that control the operation of the RAS.
3. Documentation showing that any multifunction device used to perform RAS function(s), in addition to other functions such as protective relaying or SCADA, does not compromise the reliability of the RAS when the device is not in service or is being maintained.
4. Documentation describing the System performance resulting from a single component failure in the RAS, except for limited impact RAS, when the RAS is intended to operate. A single component failure in a RAS not determined to be limited impact must not prevent the BES from meeting the same performance requirements (defined in Reliability Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed. The documentation should describe or illustrate how the design achieves this objective.
5. Documentation describing the functional testing process.

IV. RAS Retirement

The following checklist identifies RAS information that the RAS-entity shall document and provide to each reviewing RC.

1. Information necessary to ensure that the RC is able to understand the physical and electrical location of the RAS and related facilities.
2. A summary of applicable technical studies and technical justifications upon which the decision to retire the RAS is based.
3. Anticipated date of RAS retirement.

Attachment 2
Reliability Coordinator RAS Review Checklist

The following checklist identifies reliability-related considerations for the Reliability Coordinator (RC) to review and verify for each new or functionally modified[4] Remedial Action Scheme (RAS). The RC review is not limited to the checklist items and the RC may request additional information on any aspect of the RAS as well as any reliability issue related to the RAS. If a checklist item is not relevant to a particular RAS, it should be noted as "Not Applicable." If reliability considerations are identified during the review, the considerations and the proposed resolutions should be documented with the remaining applicable Attachment 2 items.

I. Design

1. The RAS actions satisfy performance objectives for the scope of events and conditions that the RAS is intended to mitigate.
2. The designed timing of RAS operation(s) is appropriate to its BES performance objectives.
3. The RAS arming conditions, if applicable, are appropriate to its System performance objectives.
4. The RAS avoids adverse interactions with other RAS, and protection and control systems.
5. The effects of RAS incorrect operation, including inadvertent operation and failure to operate, have been identified.
6. Determination whether or not the RAS is limited impact.[5] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.
7. Except for limited impact RAS as determined by the RC, the possible inadvertent operation of the RAS resulting from any single RAS component malfunction satisfies all of the following:
    a. The BES shall remain stable.
    b. Cascading shall not occur.
    c. Applicable Facility Ratings shall not be exceeded.

---

[4] Functionally modified: Any modification to a RAS consisting of any of the following:
- Changes to System conditions or contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

[5] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

d. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.

e. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.

8. The effects of future BES modifications on the design and operation of the RAS have been identified, where applicable.

II. Implementation

1. The implementation of RAS logic appropriately correlates desired actions (outputs) with events and conditions (inputs).
2. Except for limited impact RAS as determined by the RC, a single component failure in a RAS does not prevent the BES from meeting the same performance requirements as those required for the events and conditions for which the RAS is designed.
3. The RAS design facilitates periodic testing and maintenance.
4. The mechanism or procedure by which the RAS is armed is clearly described, and is appropriate for reliable arming and operation of the RAS for the conditions and events for which it is designed to operate.

III. RAS Retirement

RAS retirement reviews should assure that there is adequate justification for why a RAS is no longer needed.

Attachment 3
Database Information

1. RAS name.
2. Each RAS-entity and contact information.
3. Expected or actual in-service date; most recent RC-approval date (Requirement R3); most recent evaluation date (Requirement R4); and date of retirement, if applicable.
4. System performance issue or reason for installing the RAS (e.g., thermal overload, angular instability, poor oscillation damping, voltage instability, under- or over-voltage, or slow voltage recovery).
5. Description of the Contingencies or System conditions for which the RAS was designed (i.e., initiating conditions).
6. Action(s) to be taken by the RAS.
7. Identification of limited impact[6] RAS.
8. Any additional explanation relevant to high-level understanding of the RAS.

[6] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

Technical Justification

4.1.1 Reliability Coordinator

The Reliability Coordinator (RC) is the best-suited functional entity to perform the Remedial Action Scheme (RAS) review because the RC has the widest area reliability perspective of all functional entities and an awareness of reliability issues in neighboring RC Areas. The Wide Area purview better facilitates the evaluation of interactions among separate RAS, as well as interactions among RAS and other protection and control systems. The selection of the RC also minimizes the possibility of a conflict of interest that could exist because of business relationships among the RAS-entity, Planning Coordinator, Transmission Planner, or other entities involved in the planning or implementation of a RAS. The RC is also less likely to be a stakeholder in any given RAS and can therefore maintain objective independence.

4.1.2 Planning Coordinator

The Planning Coordinator (PC) is the best-suited functional entity to perform the RAS evaluation to verify the continued effectiveness and coordination of the RAS, its inadvertent operation performance, and the performance for a single component failure. The items that must be addressed in the evaluations include: 1) RAS mitigation of the System condition(s) or event(s) for which it was designed; 2) RAS avoidance of adverse interactions with other RAS and with protection and control systems; 3) the impact of inadvertent operation; and 4) the impact of a single component failure. The evaluation of these items involves modeling and studying the interconnected transmission system, similar to the planning analyses performed by PCs.

4.1.3 RAS-entity

The RAS-entity is any Transmission Owner, Generator Owner, or Distribution Provider that owns all or part of a RAS. If all of the RAS (RAS components) have a single owner, then that RAS-entity has sole responsibility for all the activities assigned within the standard to the RAS-entity. If the RAS (RAS components) have more than one owner, then each separate RAS component owner is a RAS-entity and is obligated to participate in various activities identified by the Requirements.

The standard does not stipulate particular compliance methods. RAS-entities have the option of collaborating to fulfill their responsibilities for each applicable requirement. Such collaboration and coordination may promote efficiency in achieving the reliability objectives of the requirements; however, the individual RAS-entity must be able to demonstrate its participation for compliance. As an example, the individual RAS-entities could collaborate to produce and submit a single, coordinated Attachment 1 to the reviewing RC pursuant to Requirement R1 to initiate the RAS review process.

Limited impact

RAS are unique and customized assemblages of protection and control equipment that vary in complexity and impact on the reliability of the BES. These differences in RAS design, action, and risk to the BES are identified and verified within the construct of Requirements R1-R4 of PRC-012-2.

The reviewing RC has the authority to designate a RAS as limited impact if the RAS cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled

separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. The reviewing RC makes the final determination as to whether a RAS qualifies for the limited impact designation based upon the studies and other information provided with the Attachment 1 submittal by the RAS-entity.

The standard recognizes the Local Area Protection Scheme (LAPS) classification in WECC (Western Electricity Coordinating Council) and the Type III classification in NPCC (Northeast Power Coordinating Council) as initially appropriate for limited impact designation. The following information describing the aforementioned WECC and NPCC RAS is excerpted from the respective regional documentation[7].The drafting team notes that the information below represents the state of the WECC and NPCC regional processes at the time of this standard development and is subject to change before the effective date of PRC-012-2.

WECC: Local Area Protection Scheme (LAPS)

A Remedial Action Scheme (RAS) whose failure to operate would NOT result in any of the following:

- Violations of TPL-001-WECC-RBP System Performance RBP,
- Maximum load loss ≥ 300 MW,
- Maximum generation loss ≥ 1000 MW.

NPCC: Type III

An SPS whose misoperation or failure to operate results in no **significant adverse impact** outside the **local area**.

The following terms are also defined by NPCC to assess the impact of the SPS for classification:

Significant adverse impact – With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:

a. system instability;

b. unacceptable system dynamic response or equipment tripping;

c. voltage levels in violation of applicable emergency limits;

d. loadings on transmission facilities in violation of applicable emergency limits;

e. unacceptable loss of load.

Local area – An electrically confined or radial portion of the system. The geographic size and number of system elements contained will vary based on system characteristics. A local area may be relatively large geographically with relatively few buses in a sparse system, or be

[7] WECC Procedure to Submit a RAS for Assessment Information Required to Assess the Reliability of a RAS Guideline, Revised 10/28/2013 | NPCC Regional Reliability Reference Directory # 7, Special Protection Systems, Version 2, 3/31/2015

relatively small geographically with a relatively large number of buses in a densely networked system.

A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional review processes of WECC or NPCC and classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type III in NPCC, is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

To propose an existing RAS (a RAS implemented prior to the effective date of PRC-012-2) be designated as limited impact by the reviewing RC, the RAS-entity must prepare and submit the appropriate Attachment 1 information that includes the technical justification (evaluations) documenting that the System can meet the performance requirements (specified in Requirement R4, Parts 4.1.4 and 4.1.5) resulting from a single RAS component malfunction or failure, respectively.

There is nothing that precludes a RAS-entity from working with the reviewing RC during the implementation period of PRC-012-2, in anticipation of the standard becoming enforceable. However, even if the reviewing RC determines the RAS qualifies as limited impact, the designation is not relevant until the standard becomes effective. Until then, the existing regional processes remain in effect as well as the existing RAS classifications or lack thereof.

An example of a scheme that could be recognized as a limited impact RAS is a load shedding or generation rejection scheme used to mitigate the overload of a BES transmission line. The inadvertent operation of such a scheme would cause the loss of either a certain amount of generation or load. The evaluation by the RAS-entity should demonstrate that the loss of this amount of generation or load, without the associated contingency for RAS operation actually occurring, is acceptable and not detrimental to the reliability of BES; e.g., in terms of frequency and voltage stability. The failure of that scheme to operate when intended could potentially lead to the overloading of a transmission line beyond its acceptable rating. The RAS-entity would need to demonstrate that this overload, while in excess of the applicable Facility Rating, is not detrimental to the BES outside the contained area (predetermined by studies) affected by the contingency.

Other examples of limited impact RAS include:

- A scheme used to protect BES equipment from damage caused by overvoltage through generation rejection or equipment tripping.
- A centrally-controlled undervoltage load shedding scheme used to protect a contained area (predetermined by studies) of the BES against voltage collapse.
- A scheme used to trip a generating unit following certain BES Contingencies to prevent the unit from going out of synch with the System; where, if the RAS fails to operate and the unit pulls out of synchronism, the resulting apparent impedance swings do not

result in the tripping of any Transmission System Elements other than the generating unit and its directly connected Facilities.

Requirement R1

Each RAS is unique and its action(s) can have a significant impact on the reliability and integrity of the Bulk Electric System (BES); therefore, a review of a proposed new RAS or an existing RAS proposed for functional modification, or retirement (removal from service) must be completed prior to implementation.

Functional modifications consists of any of the following:

- Changes to System conditions or Contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

An example indicating the limits of an in-kind replacement of a RAS component is the replacement of one relay (or other device) with a relay (or other device) that uses similar functions. For instance, if a RAS included a CO-11 relay which was replaced by an IAC-53 relay, that would be an in-kind replacement. If the CO-11 relay were replaced by a microprocessor SEL-451 relay that used only the same functions as the original CO-11 relay, that would also be an in-kind replacement; however, if the SEL-451 relay was used to add new logic to what the CO-11 relay had provided, then the replacement relay would be a functional modification.

Changes to RAS pickup levels that require no other scheme changes are not considered a functional modification. For example, System conditions require a RAS to be armed when the combined flow on two lines exceeds 500 MW. If a periodic evaluation pursuant to Requirement R4, or other assessment, indicates that the arming level should be reduced to 450 MW without requiring any other RAS changes that would not be a functional modification. Similarly, if a RAS is designed to shed load to reduce loading on a particular line below 1000 amps, then a change in the load shedding trigger from 1000 amps to 1100 amps would not be a functional modification.

Another example illustrates a case where a System change may result in a RAS functional change. Assume that a generation center is connected to a load center through two transmission lines. The lines are not rated to accommodate full plant output if one line is out of service, so a RAS monitors the status of both lines and trips or ramps down the generation to a safe level following loss of either line. Later, one of the lines is tapped to serve additional load. The System that the RAS impacts now includes three lines, loss of any of which is likely to still require generation reduction. The modified RAS will need to monitor all three lines (add two line terminal status inputs to the RAS) and the logic to recognize the specific line outages would

change, while the generation reduction (RAS output) requirement may or may not change, depending on which line is out of service. These required RAS changes would be a functional modification.

Any functional modification to a RAS will need to be reviewed and approved through the process described in Requirements R1, R2, and R3. The need for such functional modifications may be identified in several ways including but not limited to the Planning evaluations pursuant to R4, incorrect operations pursuant to R5, a test failure pursuant to R8, or Planning assessments related to future additions or modifications of other facilities.

See Item 4a in the Implementation Section of Attachment 1 in the Supplemental Material section for typical RAS components for which a failure may be considered. The RC has the discretion to make the final determination regarding which components should be regarded as RAS components during its review.

To facilitate a review that promotes reliability, the RAS-entity(ies) must provide the reviewer with sufficient details of the RAS design, function, and operation. This data and supporting documentation are identified in Attachment 1 of this standard, and Requirement R1 mandates that the RAS-entity(ies) provide them to the reviewing Reliability Coordinator (RC). The RC that coordinates the area where the RAS is located is responsible for the review. In cases where a RAS crosses multiple RC Area boundaries, each affected RC is responsible for conducting either individual reviews or a coordinated review.

Requirement R1 does not specify how far in advance of implementation the RAS-entity(ies) must provide Attachment 1 data to the reviewing RC. The information will need to be submitted early enough to allow RC review in the allotted time pursuant to Requirement R2, including resolution of any reliability issues that might be identified, in order to obtain approval of the reviewing RC. Expeditious submittal of this information is in the interest of each RAS-entity to effect a timely implementation.

Requirement R2

Requirement R2 mandates that the RC perform reviews of all proposed new RAS and existing RAS proposed for functional modification, or retirement (removal from service) in its RC Area.

RAS are unique and customized assemblages of protection and control equipment. As such, they have a potential to introduce reliability risks to the BES, if not carefully planned, designed, and installed. A RAS may be installed to address a reliability issue, or achieve an economic or operational advantage, and could introduce reliability risks that might not be apparent to a RAS-entity(ies). An independent review by a multi-disciplinary panel of subject matter experts with planning, operations, protection, telecommunications, and equipment expertise is an effective means of identifying risks and recommending RAS modifications when necessary.

The RC is the functional entity best suited to perform the RAS reviews because it has the widest area reliability perspective of all functional entities and an awareness of reliability issues in

neighboring RC Areas. This Wide Area purview facilitates the evaluation of interactions among separate RAS as well as interactions among the RAS and other protection and control systems.

The selection of the RC also minimizes the possibility of a "conflict of interest" that could exist because of business relationships among the RAS-entity, Planning Coordinator (PC), Transmission Planner (TP), or other entities that are likely to be involved in the planning or implementation of a RAS. The RC may request assistance in RAS reviews from other parties such as the PC(s) or regional technical groups (e.g., Regional Entities); however, the RC retains responsibility for compliance with the requirement. It is recognized that the RC does not possesses more information or ability than anticipated by their functional registration as designated by NERC. The NERC Functional Model is a guideline for the development of standards and their applicability and does not contain compliance requirements. If Reliability Standards address functions that are not described in the model, the Reliability Standard requirements take precedence over the Functional Model. For further reference, please see the Introduction section of NERC's Reliability Functional Model, Version 5, November 2009. Attachment 2 of this standard is a checklist for assisting the RC in identifying design and implementation aspects of a RAS, and for facilitating consistent reviews of each RAS submitted for review. The time frame of four full calendar months is consistent with current utility practice; however, flexibility is provided by allowing the parties to negotiate a different schedule for the review. Note, an RC may need to include this task in its reliability plan(s) for the NERC Region(s) in which it is located.

Requirement R3

Requirement R3 mandates that each RAS-entity resolve all reliability issues (pertaining to its RAS) identified during the RAS review by the reviewing Reliability Coordinators. Examples of reliability issues include a lack of dependability, security, or coordination. RC approval of a RAS is considered to be obtained when the reviewing RC's feedback to each RAS-entity indicates that either no reliability issues were identified during the review or all identified reliability issues were resolved to the RC's satisfaction.

Dependability is a component of reliability that is the measure of certainty of a device to operate when required. If a RAS is installed to meet performance requirements of NERC Reliability Standards, a failure of the RAS to operate when intended would put the System at risk of violating NERC Reliability Standards if specified Contingency(ies) or System conditions occur. This risk is mitigated by designing the RAS so that it will accomplish the intended purpose while experiencing a single RAS component failure. This is often accomplished through redundancy. Other strategies for providing dependability include "over-tripping" load or generation, or alternative automatic backup schemes.

Security is a component of reliability that is the measure of certainty of a device to not operate inadvertently. False or inadvertent operation of a RAS results in taking a programmed action without the appropriate arming conditions, occurrence of specified Contingency(ies), or System conditions expected to trigger the RAS action. Typical RAS actions include shedding load or generation or re-configuring the System. Such actions, if inadvertently taken, are undesirable

and may put the System in a less secure state. Worst case impacts from inadvertent operation often occur if all programmed RAS actions occur. If the System performance still satisfies PRC-012-2 Requirement R4, Part 4.3, no additional mitigation is required. Security enhancements to the RAS design, such as voting schemes, are acceptable mitigations against inadvertent operations.

Any reliability issue identified during the review must be resolved before implementing the RAS to avoid placing the System at unacceptable risk. The RAS-entity or the reviewing RC(s) may have alternative ideas or methods available to resolve the issue(s). In either case, the concern needs to be resolved in deference to reliability, and the RC has the final decision.

A specific time period for the RAS-entity to respond to the RC(s) review is not necessary because an expeditious response is in the interest of each RAS-entity to effect a timely implementation.

A specific time period for the RC to respond to the RAS-entity following the RAS review is also not necessary because the RC will be aware of (1) any reliability issues associated with the RAS not being in service and (2) the RAS-entity's schedule to implement the RAS to address those reliability issues. Since the RC is the ultimate arbiter of BES operating reliability, resolving reliability issues is a priority for the RC and serves as an incentive to expeditiously respond to the RAS-entity.

Requirement R4

Requirement R4 mandates that an evaluation of each RAS be performed at least once every five full calendar years. The purpose of a periodic RAS evaluation is to verify the continued effectiveness and coordination of the RAS, as well as to verify that requirements for BES performance following inadvertent RAS operation and single component failure continue to be satisfied. A periodic evaluation is required because changes in System topology or operating conditions may change the effectiveness of a RAS or the way it interacts with and impacts the BES.

A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. Limited impact RAS are not subject to the RAS single component malfunction and failure tests of Parts 4.1.4 and 4.1.5, respectively. Requiring a limited impact RAS to meet these tests would add complexity to the design with minimal benefit to BES reliability.

A RAS implemented after the effective date of this standard can only be designated as limited impact by the reviewing RC(s). A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional review processes of WECC or NPCC and is classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type III in NPCC is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

Requirement R4 also clarifies that the RAS single component failure and inadvertent operation tests do not apply to RAS which are determined to be limited impact. Requiring a limited impact RAS to meet the single component failure and inadvertent operation tests would just add complexity to the design with little or no improvement in the reliability of the BES.

For existing RAS, the initial performance of Requirement R4 must be completed within five full calendar years of the effective date of PRC-012-2. For new or functionally modified RAS, the initial performance of the requirement must be completed within five full calendar years of the RAS approval date by the reviewing RC(s). Five full calendar years was selected as the maximum time frame between evaluations based on the time frames for similar requirements in Reliability Standards PRC-006, PRC-010, and PRC-014. The RAS evaluation can be performed sooner if it is determined that material changes to System topology or System operating conditions could potentially impact the effectiveness or coordination of the RAS. System changes also have the potential to alter the reliability impact of limited impact RAS on the BES. Requirement 4, Part 4.1.3 explicitly requires the periodic evaluation of limited impact RAS to verify the limited impact designation remains applicable. The periodic RAS evaluation will typically lead to one of the following outcomes: 1) affirmation that the existing RAS is effective; 2) identification of changes needed to the existing RAS; or, 3) justification for RAS retirement.

The items required to be addressed in the evaluations (Requirement R4, Parts 4.1.1 through 4.1.5) are planning analyses that may involve modeling of the interconnected transmission system to assess BES performance. The PC is the functional entity best suited to perform the analyses because they have a wide-area planning perspective. To promote reliability, the PC is required to provide the results of the evaluation to each impacted Transmission Planner and Planning Coordinator, in addition to each reviewing RC and RAS-entity. In cases where a RAS crosses PC boundaries, each affected PC is responsible for conducting either individual evaluations or participating in a coordinated evaluation.

The intent of Requirement R4, Part 4.1.4 is to verify that the possible inadvertent operation of the RAS (other than limited impact RAS), caused by the malfunction of a single component of the RAS, meet the same System performance requirements as those required for the Contingency(ies) or System conditions for which it is designed. If the RAS is designed to meet one of the planning events (P0-P7) in TPL-001-4, the possible inadvertent operation of the RAS must meet the same performance requirements listed in the standard for that planning event. The requirement clarifies that the inadvertent operation to be considered is only that caused by the malfunction of a single RAS component. This allows features to be designed into the RAS to improve security, such that inadvertent operation due to malfunction of a single component is prevented; otherwise, the RAS inadvertent operation must satisfy Requirement R4, Part 4.1.4.

The intent of Requirement R4, Part 4.1.4 is also to verify that the possible inadvertent operation of the RAS (other than limited impact RAS) installed for an extreme event in TPL-001-4 or for some other Contingency or System conditions not defined in TPL-001-4 (therefore without performance requirements), meet the minimum System performance requirements of Category P7 in Table 1 of NERC Reliability Standard TPL-001-4. However, instead of referring to the TPL

standard, the requirement lists the System performance requirements that a potential inadvertent operation must satisfy. The performance requirements listed (Requirement R4, Parts 4.1.4.1 – 4.1.4.5) are the ones that are common to all planning events (P0-P7) listed in TPL-001-4.

With reference to Requirement 4, Part 4.1.4, note that the only differences in performance requirements among the TPL (P0-P7) events (not common to all of them) concern Non-Consequential Load Loss and interruption of Firm Transmission Service. It is not necessary for Requirement R4, Part 4.1.4 to specify performance requirements related to these areas because a RAS is only allowed to drop non-consequential load or interrupt Firm Transmission Service if that action is allowed for the Contingency for which it is designed. Therefore, the inadvertent operation should automatically meet Non-Consequential Load Loss or interrupting Firm Transmission Service performance requirements for the Contingency(ies) for which it was designed.

The intent of Requirement R4, Part 4.1.5 is to verify that a single component failure in a RAS, other than limited impact RAS, when the RAS is intended to operate, does not prevent the BES from meeting the same performance requirements (defined in Reliability Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed. This analysis is needed to ensure that changing System conditions do not result in the single component failure requirement not being met.

The following is an example of a single component failure causing the System to fail to meet the performance requirements for the P1 event for which the RAS was installed. Consider the instance where a three-phase Fault (P1 event) results in a generating plant becoming unstable (a violation of the System performance requirements of TPL-001-4). To resolve this, a RAS is installed to trip a single generating unit which allows the remaining units at the plant to remain stable. If failure of a single component (e.g., relay) in the RAS results in the RAS failing to operate for the P1 event, the generating plant would become unstable (failing to meet the System performance requirements of TPL-001-4 for a P1 event).

Requirement R4, Part 4.1.5 does not mandate that all RAS have redundant components. For example:

- Consider the instance where a RAS is installed to mitigate an extreme event in TPL-001-4. There are no System performance requirements for extreme events; therefore, the RAS does not need redundancy to meet the same performance requirements as those required for the events and conditions for which the RAS was designed.

- Consider a RAS that arms more load or generation than necessary such that failure of the RAS to drop a portion of load or generation due to that single component failure will still result in satisfactory System performance, as long as tripping the total armed amount of load or generation does not cause other adverse impacts to reliability.

The scope of the periodic evaluation does not include a new review of the physical implementation of the RAS, as this was confirmed by the RC during the initial review and verified by subsequent functional testing. However, it is possible that a RAS design which previously satisfied requirements for inadvertent RAS operation and single component failure by means other than component redundancy may fail to satisfy these requirements at a later time, and must be evaluated with respect to the current System. For example, if the actions of a particular RAS include tripping load, load growth could occur over time that impacts the amount of load to be tripped. These changes could result in tripping too much load upon inadvertent operation and result in violations of Facility Ratings. Alternatively, the RAS might be designed to trip more load than necessary (i.e., "over trip") in order to satisfy single component failure requirements. System changes could result in too little load being tripped and unacceptable BES performance if one of the loads failed to trip.

Requirement R5

The correct operation of a RAS is important to maintain the reliability and integrity of the BES. Any incorrect operation of a RAS indicates the RAS effectiveness and/or coordination may have been compromised. Therefore, all operations of a RAS and failures of a RAS to operate when expected must be analyzed to verify that the RAS operation was consistent with its intended functionality and design.

A RAS operational performance analysis is intended to: (1) verify RAS operation is consistent with implemented design; or (2) identify RAS performance deficiencies that manifested in the incorrect RAS operation or failure of RAS to operate when expected.

The 120 full calendar day time frame for the completion of RAS operational performance analysis aligns with the time frame established in Requirement R1 from PRC-004-4 regarding the investigation of a Protection System Misoperation; however, flexibility is provided by allowing the parties to negotiate a different schedule for the analysis. To promote reliability, the RAS-entity(s) is required to provide the results of RAS operational performance analyses to its reviewing RC(s) if the analyses revealed a deficiency.

The RAS-entity(ies) may need to collaborate with its associated Transmission Planner to comprehensively analyze RAS operational performance. This is because a RAS operational performance analysis involves verifying that the RAS operation was triggered correctly (Part 5.1.1), responded as designed (Part 5.1.2), and that the resulting BES response (Parts 5.1.3 and 5.1.4) was consistent with the intended functionality and design of the RAS. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to conduct and submit a single, coordinated operational performance analysis.

Requirement R6

RAS deficiencies potentially pose a reliability risk to the BES. RAS deficiencies may be identified in the periodic RAS evaluation conducted by the PC in Requirement R4, in the operational analysis conducted by the RAS-entity in Requirement R5, or in the functional test performed by the RAS-entity(ies) in Requirement R8. To mitigate potential reliability risks, Requirement R6

mandates that each RAS-entity participate in developing a CAP that establishes the mitigation actions and timetable necessary to address the deficiency.

The RAS-entity(ies) that owns the RAS components, is responsible for the RAS equipment, and is in the best position to develop the timelines and perform the necessary work to correct RAS deficiencies. If necessary, the RAS-entity(ies) may request assistance with development of the CAP from other parties such as its Transmission Planner or Planning Coordinator; however, the RAS-entity has the responsibility for compliance with this requirement.

A CAP may require functional changes be made to a RAS. In this case, Attachment 1 information must be submitted to the reviewing RC(s), an RC review must be performed to obtain RC approval before the RAS-entity can place RAS modifications in service, per Requirements R1, R2, and R3.

Depending on the complexity of the issues, development of a CAP may require study, engineering or consulting work. A timeframe of six full calendar months is allotted to allow enough time for RAS-entity collaboration on the CAP development, while ensuring that deficiencies are addressed in a reasonable time. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to develop and submit a single, coordinated CAP. A RAS deficiency may require the RC or Transmission Operator to impose operating restrictions so the System can operate in a reliable way until the RAS deficiency is resolved. The possibility of such operating restrictions will incent the RAS-entity to resolve the issue as quickly as possible.

The following are example situations of when a CAP is required:

- A determination after a RAS operation/non-operation investigation that the RAS did not meet performance expectations or did not operate as designed.
- Periodic planning assessment reveals RAS changes are necessary to correct performance or coordination issues.
- Equipment failures.
- Functional testing identifies that a RAS is not operating as designed.

Requirement R7

Requirement R7 mandates that each RAS-entity implement its CAP developed in Requirement R6 which mitigates the deficiencies identified in Requirements R4, R5, or R8. By definition, a CAP is: “A list of actions and an associated timetable for implementation to remedy a specific problem.”

A CAP can be modified if necessary to account for adjustments to the actions or scheduled timetable of activities. If the CAP is changed, the RAS-entity must notify the reviewing Reliability

Coordinator(s). The RAS-entity must also notify the Reliability Coordinator(s) when the CAP has been completed.

The implementation of a properly developed CAP ensures that RAS deficiencies are mitigated in a timely manner. A RAS deficiency may require the RC or Transmission Operator to impose operating restrictions so the System can operate in a reliable way until the CAP is completed. The possibility of such operating restrictions will incent the RAS-entity to complete the CAP as quickly as possible.

Requirement R8

The reliability objective of Requirement R8 is to test the non-Protection System components of a RAS (controllers such as programmable logic controllers (PLCs)) and to verify the overall performance of the RAS through functional testing. Functional tests validate RAS operation by ensuring System states are detected and processed, and that actions taken by the controls are correct and occur within the expected time using the in-service settings and logic. Functional testing is aimed at assuring overall RAS performance and not the component focused testing contained in the PRC-005 maintenance standard.

Since the functional test operates the RAS under controlled conditions with known System states and expected results, testing and analysis can be performed with minimum impact to the BES and should align with expected results. The RAS-entity is in the best position to determine the testing procedure and schedule due to their overall knowledge of the RAS design, installation, and functionality. Periodic testing provides the RAS-entity assurance that latent failures may be identified and also promotes identification of changes in the System that may have introduced latent failures.

The six and twelve full calendar year functional testing intervals are greater than the annual or bi-annual periodic testing performed in some NERC Regions. However, these intervals are a balance between the resources required to perform the testing and the potential reliability impacts to the BES created by undiscovered latent failures that could cause an incorrect operation of the RAS. Longer test intervals for limited impact RAS are acceptable because incorrect operations or failures to operate present a low reliability risk to the Bulk Power System.

Functional testing is not synonymous with end-to-end testing. End-to-end testing is an acceptable method but may not be feasible for many RAS. When end-to-end testing is not possible, a RAS-entity may use a segmented functional testing approach. The segments can be tested individually negating the need for complex maintenance schedules. In addition, actual RAS operation(s) can be used to fulfill the functional testing requirement. If a RAS does not operate in its entirety during a System event or System conditions do not allow an end-to-end scheme test, then the segmented approach should be used to fulfill this Requirement. Functional testing includes the testing of all RAS inputs used for detection, arming, operating, and data collection. Functional testing, by default operates the processing logic and infrastructure of a RAS, but focuses on the RAS inputs as well as the actions initiated by RAS

outputs to address the System condition(s) for which the RAS is designed. All segments and components of a RAS must be tested or have proven operations within the applicable maximum test interval to demonstrate compliance with the Requirement.

As an example of segment testing, consider a RAS controller implemented using a PLC that receives System data, such as loading or line status, from distributed devices. These distributed devices could include meters, protective relays, or other PLCs. In this example RAS, a line protective relay is used to provide an analog metering quantity to the RAS control PLC. A functional test would verify that the System data is received from the protective relay by the PLC, processed by the PLC, and that PLC outputs are appropriate. There is no need to verify the protective relay's ability to measure the power system quantities, as this is a requirement for Protection Systems used as RAS in PRC-005, Table 1-1, Component Type – Protective Relay. Rather the functional test is focused on the use of the protective relay data at the PLC, including the communications data path from relay to PLC if this data is essential for proper RAS operation. Additionally, if the control signal back to the protective relay is also critical to the proper functioning of this example RAS, then that path is also verified up to the protective relay. This example describes a test for one segment of a RAS which verifies RAS action, verifies PLC control logic, and verifies RAS communications.

IEEE C37.233, "IEEE Guide for Power System Protection Testing," 2009 section 8 (particularly 8.3-8.5), provides an overview of functional testing. The following opens section 8.3:

> Proper implementation requires a well-defined and coordinated test plan for performance evaluation of the overall system during agreed maintenance intervals. The maintenance test plan, also referred to as functional system testing, should include inputs, outputs, communication, logic, and throughput timing tests. The functional tests are generally not component-level testing, rather overall system testing. Some of the input tests may need to be done ahead of overall system testing to the extent that the tests affect the overall performance. The test coordinator or coordinators need to have full knowledge of the intent of the scheme, isolation points, simulation scenarios, and restoration to normal procedures.
>
> The concept is to validate the overall performance of the scheme, including the logic where applicable, to validate the overall throughput times against system modeling for different types of Contingencies, and to verify scheme performance as well as the inputs and outputs.

If a RAS passes a functional test, it is not necessary to provide that specific information to the RC because that is the expected result and requires no further action. If a segment of a RAS fails a functional test, the status of that degraded RAS is required to be reported (in Real-time) to the Transmission Operator via PRC-001, Requirement R6, then to the RC via TOP-001-3, Requirement R8. See Phase 2 of Project 2007-06 for the mapping document from PRC-001 to other standards regarding notification of RC by TOP if a deficiency is found during testing. Consequently, it is not necessary to include a similar requirement in this standard.

The initial test interval begins on the effective date of the standard pursuant to the implementation plan. Subsequently, the maximum allowable interval between functional tests

is six full calendar years for RAS that are not designated as limited impact RAS and twelve full calendar years for RAS that are designated as limited impact RAS. The interval between tests begins on the date of the most recent successful test for each individual segment or end-to-end test. A successful test of one segment only resets the test interval clock for that segment. A RAS-entity may choose to count a correct RAS operation as a qualifying functional test for those RAS segments which operate. If a System event causes a correct, but partial RAS operation, separate functional tests of the segments that did not operate are still required within the maximum test interval that started on the date of the previous successful test of those (non-operating) segments in order to be compliant with Requirement R8.

Requirement R9

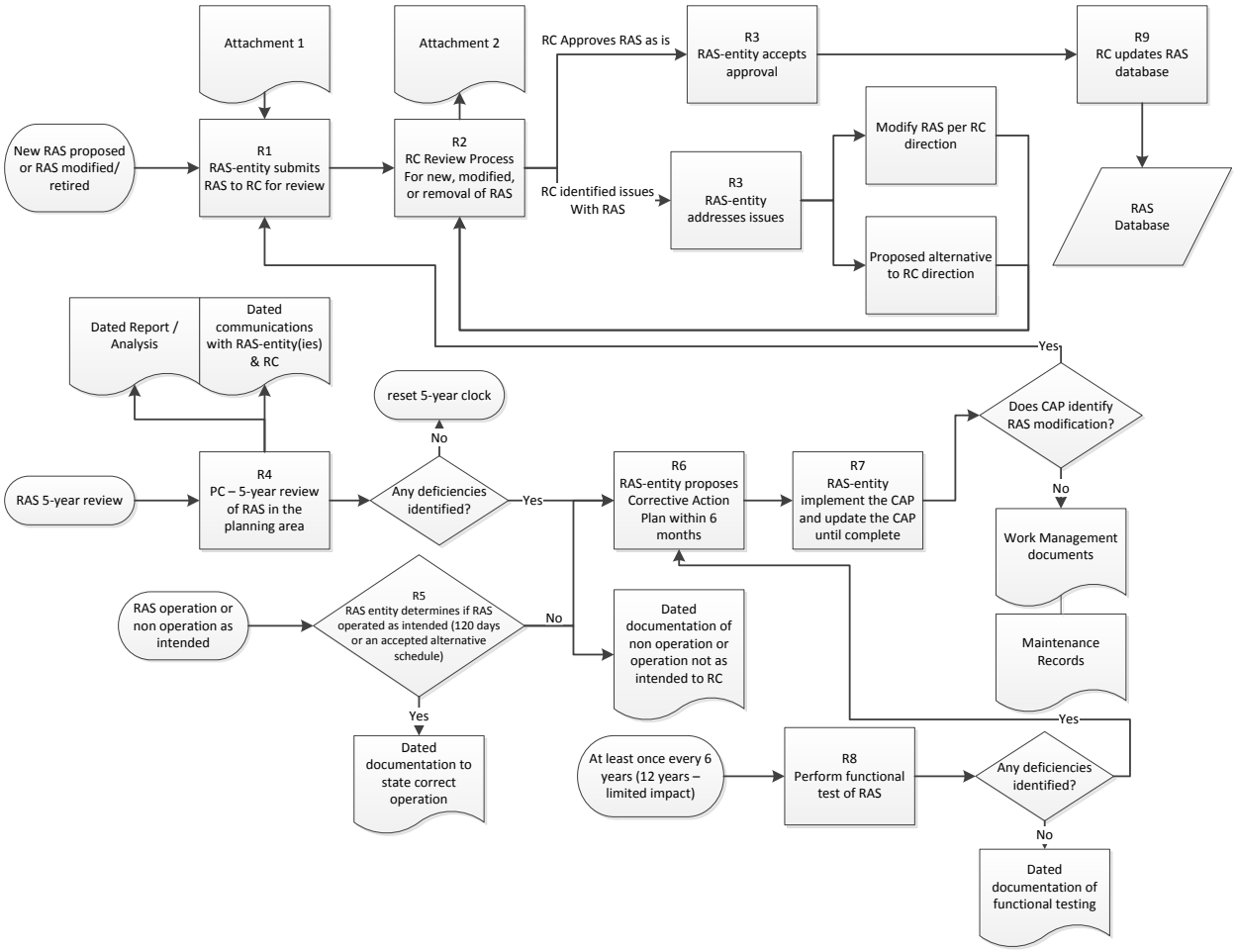
The RAS database required to be maintained by the RC in Requirement R9 ensures information regarding existing RAS is available. Attachment 3 contains the minimum information that is required to be included about each RAS listed in the database. Additional information can be requested by the RC.

The database enables the RC to provide other entities high-level information on existing RAS that could potentially impact the operational and/or planning activities of that entity. The information provided is sufficient for an entity with a reliability need to evaluate whether the RAS can impact its System. For example, a RAS performing generation rejection to mitigate an overload on a transmission line may cause a power flow change within an adjacent entity area. This entity should be able to evaluate the risk that a RAS poses to its System from the high-level information provided in the RAS database.

The RAS database does not need to list detailed settings or modeling information, but the description of the System performance issues, System conditions, and the intended corrective actions must be included. If additional details about the RAS operation are required, the entity may obtain the contact information of the RAS-entity from the RC.

Process Flow Diagram

The diagram below depicts the process flow of the PRC-012-2 requirements.



Technical Justifications for Attachment 1 Content
Supporting Documentation for RAS Review

To perform an adequate review of the expected reliability implications of a Remedial Action Scheme (RAS), it is necessary for the RAS-entity(ies) to provide a detailed list of information describing the RAS to the reviewing RC. If there are multiple RAS-entities for a single RAS, information will be needed from all RAS-entities. Ideally, in such cases, a single RAS-entity will take the lead to compile all the data identified into a single Attachment 1.

The necessary data ranges from a general overview of the RAS to summarized results of transmission planning studies, to information about hardware used to implement the RAS. Coordination between the RAS and other RAS and protection and control systems will be examined for possible adverse interactions. This review can include wide-ranging electrical design issues involving the specific hardware, logic, telecommunications, and other relevant equipment and controls that make up the RAS.

Attachment 1

The following checklist identifies important RAS information for each new or functionally modified[8] RAS that the RAS-entity shall document and provide to the RC for review pursuant to Requirement R1. When a RAS has been previously reviewed, only the proposed modifications to that RAS require review; however, it will be helpful to each reviewing RC if the RAS-entity provides a summary of the existing RAS functionality.

I. General

1. Information such as maps, one-line drawings, substation and schematic drawings that identify the physical and electrical location of the RAS and related facilities.

   Provide a description of the RAS to give an overall understanding of the functionality and a map showing the location of the RAS. Identify other protection and control systems requiring coordination with the RAS. See RAS Design below for additional information.

   Provide a single-line drawing(s) showing all sites involved. The drawing(s) should provide sufficient information to allow the RC review team to assess design reliability, and should include information such as the bus arrangement, circuit breakers, the associated switches, etc. For each site, indicate whether detection, logic, action, or a combination of these is present.

[8] Functionally modified: Any modification to a RAS consisting of any of the following:
- Changes to System conditions or contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

2. Functionality of new RAS or proposed functional modifications to existing RAS and documentation of the pre- and post-modified functionality of the RAS.
3. The Corrective Action Plan (CAP) if RAS modifications are proposed in a CAP. [Reference NERC Reliability Standard PRC-012-2, Requirements R5 and R7]

   Provide a description of any functional modifications to a RAS that are part of a CAP that are proposed to address performance deficiency(ies) identified in the periodic evaluation pursuant to Requirement R4, the analysis of an actual RAS operation pursuant to Requirement R5, or functional test failure pursuant to Requirement R8. A copy of the most recent CAP must be submitted in addition to the other data specified in Attachment 1.
4. Initial data to populate the RAS database.
   a. RAS name.
   b. Each RAS-entity and contact information.
   c. Expected or actual in-service date; most recent (Requirement R3) RC-approval date; most recent five full calendar year (Requirement R4) evaluation date; and, date of retirement, if applicable.
   d. System performance issue or reason for installing the RAS (*e.g.*, thermal overload, angular instability, poor oscillation damping, voltage instability, under-/over-voltage, slow voltage recovery).
   e. Description of the Contingencies or System conditions for which the RAS was designed (initiating conditions).
   f. Corrective action taken by the RAS.
   g. Identification of limited impact[9] RAS.
   h. Any additional explanation relevant to high level understanding of the RAS.

      Note: This is the same information as is identified in Attachment 3. Supplying the data at this point in the review process ensures a more complete review and minimizes any administrative burden on the reviewing RC(s).

II. Functional Description and Transmission Planning Information

1. Contingencies and System conditions that the RAS is intended to remedy. [Reference NERC Reliability Standards PRC-012, R1.2 and PRC-013, R1.1]
   a. The System conditions that would result if no RAS action occurred should be identified.

[9] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

b. Include a description of the System conditions that should arm the RAS so as to be ready to take action upon subsequent occurrence of the critical System Contingencies or other operating conditions when RAS action is intended to occur. If no arming conditions are required, this should also be stated.

c. Event-based RAS are triggered by specific Contingencies that initiate mitigating action. Condition-based RAS may also be initiated by specific Contingencies, but specific Contingencies are not always required. These triggering Contingencies and/or conditions should be identified.

2. The actions to be taken by the RAS in response to disturbance conditions. [Reference NERC Reliability Standards PRC-012, R1.2 and PRC-013, R1.2]

   Mitigating actions are designed to result in acceptable System performance. These actions should be identified, including any time constraints and/or "backup" mitigating measures that may be required in case of a single RAS component failure.

3. A summary of technical studies, if applicable, demonstrating that the proposed RAS actions satisfy System performance objectives for the scope of System events and conditions that the RAS is intended to remedy. The technical studies summary shall also include information such as the study year(s), System conditions, and Contingencies analyzed on which the RAS design is based, and the date those technical studies were performed. [Reference NEC Reliability Standard PRC-014, R3.2]

   Review the scheme purpose and impact to ensure it is (still) necessary, serves the intended purposes, and meets current performance requirements. While copies of the full, detailed studies may not be necessary, any abbreviated descriptions of the studies must be detailed enough to allow the reviewing RC(s) to be convinced of the need for the scheme and the results of RAS-related operations.

4. Information regarding any future System plans that will impact the RAS. [Reference NERC Reliability Standard PRC-014, R3.2]

   The RC's other responsibilities under the NERC Reliability Standards focus on the Operating Horizon, rather than the Planning Horizon. As such, the RC is less likely to be aware of any longer range plans that may have an impact on the proposed RAS. Such knowledge of future Plans is helpful to provide perspective on the capabilities of the RAS.

5. RAS-entity proposal and justification for limited impact designation, if applicable.

   A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional review processes of WECC or NPCC and is classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type 3 in NPCC is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

6. Documentation describing the System performance resulting from the possible inadvertent operation of the RAS, except for limited impact RAS, caused by any single RAS component malfunction. Single component malfunctions in a RAS not determined to be limited impact must satisfy all of the following:
   [Reference NERC Reliability Standard PRC-012, R1.4]

   a. The BES shall remain stable.

   b. Cascading shall not occur.

   c. Applicable Facility Ratings shall not be exceeded.

   d. BES voltages shall be within post-Contingency voltage limits and post-Contingency voltage deviation limits as established by the Transmission Planner and the Planning Coordinator.

   e. Transient voltage responses shall be within acceptable limits as established by the Transmission Planner and the Planning Coordinator.

7. An evaluation indicating that the RAS settings and operation avoids adverse interactions with other RAS, and protection and control systems.
   [Reference NERC Reliability Standards PRC-012, R1.5 and PRC-014, R3.4]

   RAS are complex schemes that may take action such as tripping load or generation or re-configuring the System. Many RAS depend on sensing specific System configurations to determine whether they need to arm or take actions. An examples of an adverse interaction: A RAS that reconfigures the System also changes the available Fault duty, which can affect distance relay overcurrent ("fault detector") supervision and ground overcurrent protection coordination.

8. Identification of other affected RCs.

   This information is needed to aid in information exchange among all affected entities and coordination of the RAS with other RAS and protection and control systems.

III. Implementation

1. Documentation describing the applicable equipment used for detection, dc supply, communications, transfer trip, logic processing, control actions, and monitoring.

   Detection

   Detection and initiating devices, whether for arming or triggering action, should be designed to be secure. Several types of devices have been commonly used as disturbance, condition, or status detectors:

   - Line open status (event detectors),
   - Protective relay inputs and outputs (event and parameter detectors),
   - Transducer and IED (analog) inputs (parameter and response detectors),
   - Rate of change (parameter and response detectors).

   DC Supply

Batteries and charges, or other forms of dc supply for RAS, are commonly also used for Protection Systems. This is acceptable, and maintenance of such supplies is covered by PRC-005. However, redundant RAS, when used, should be supplied from separately protected (fused or breakered) circuits.

Communications: Telecommunications Channels

Telecommunications channels used for sending and receiving RAS information between sites and/or transfer trip devices should meet at least the same criteria as other relaying protection communication channels. Discuss performance of any non-deterministic communication systems used (such as Ethernet).

The scheme logic should be designed so that loss of the channel, noise, or other channel or equipment failure will not result in a false operation of the scheme.

It is highly desirable that the channel equipment and communications media (power line carrier, microwave, optical fiber, etc.) be owned and maintained by the RAS-entity, or perhaps leased from another entity familiar with the necessary reliability requirements. All channel equipment should be monitored and alarmed to the dispatch center so that timely diagnostic and repair action shall take place upon failure. Publicly switched telephone networks are generally an undesirable option.

Communication channels should be well labeled or identified so that the personnel working on the channel can readily identify the proper circuit. Channels between entities should be identified with a common name at all terminals.

Transfer Trip

Transfer trip equipment, when separate from other RAS equipment, should be monitored and labeled similarly to the channel equipment.

Logic Processing

All RAS require some form of logic processing to determine the action to take when the scheme is triggered. Required actions are always scheme dependent. Different actions may be required at different arming levels or for different Contingencies. Scheme logic may be achievable by something as simple as wiring a few auxiliary relay contacts or by much more complex logic processing.

Platforms that have been used reliably and successfully include PLCs in various forms, personal computers (PCs), microprocessor protective relays, remote terminal units (RTUs), and logic processors. Single-function relays have been used historically to implement RAS, but this approach is now less common except for very simple new RAS or minor additions to existing RAS.

Control Actions

RAS action devices may include a variety of equipment such as transfer trip, protective relays, and other control devices. These devices receive commands from the logic processing function (perhaps through telecommunication facilities) and initiate RAS actions at the sites where action is required.

Monitoring by SCADA/EMS should include at least

- Whether the scheme is in service or out of service.
    - For RAS that are armed manually, the arming status may be the same as whether the RAS is in service or out of service.

  - For RAS that are armed automatically, these two states are independent because a RAS that has been placed in service may be armed or unarmed based on whether the automatic arming criteria have been met.
- The current operational state of the scheme (available or not).
- In cases where the RAS requires single component failure performance; e.g., redundancy, the minimal status indications should be provided separately for each RAS.
  - The minimum status is generally sufficient for operational purposes; however, where possible it is often useful to provide additional information regarding partial failures or the status of critical components to allow the RAS-entity to more efficiently troubleshoot a reported failure. Whether this capability exists will depend in part on the design and vintage of equipment used in the RAS. While all schemes should provide the minimum level of monitoring, new schemes should be designed with the objective of providing monitoring at least similar to what is provided for microprocessor-based Protection Systems.

2. Information on detection logic and settings/parameters that control the operation of the RAS. [Reference NERC Reliability Standards PRC-012, R1.2 and PRC-013, R1.3]

   Several methods to determine line or other equipment status are in common use, often in combination:

   a. Auxiliary switch contacts from circuit breakers and disconnect switches (52a/b, 89a/b)—the most common status monitor; “a” contacts exactly emulate actual breaker status, while “b” contacts are opposite to the status of the breaker;

   b. Undercurrent detection—a low level indicates an open condition, including at the far end of a line; pickup is typically slightly above the total line-charging current;

   c. Breaker trip coil current monitoring—typically used when high-speed RAS response is required, but usually in combination with auxiliary switch contacts and/or other detection because the trip coil current ceases when the breaker opens; and

   d. Other detectors such as angle, voltage, power, frequency, rate of change of the aforementioned, out of step, etc. are dependent on specific scheme requirements, but some forms may substitute for or enhance other monitoring described in items ‘a’, ‘b’, and ‘c’ above.

   Both RAS arming and action triggers often require monitoring of analog quantities such as power, current, and voltage at one or more locations and are set to detect a specific level of the pertinent quantity. These monitors may be relays, meters, transducers, or other devices

3. Documentation showing that any multifunction device used to perform RAS function(s), in addition to other functions such as protective relaying or SCADA, does not compromise the reliability of the RAS when the device is not in service or is being maintained.

In this context, a multifunction device (e.g., microprocessor-based relay) is a single component that is used to perform the function of a RAS in addition to protective relaying and/or SCADA simultaneously. It is important that other applications in the multifunction device do not compromise the functionality of the RAS when the device is in service or when it is being maintained. The following list outlines considerations when the RAS function is applied in the same microprocessor-based relay as equipment protection functions:

a. Describe how the multifunction device is applied in the RAS.

b. Show the general arrangement and describe how the multi-function device is labeled in the design and application, so as to identify the RAS and other device functions.

c. Describe the procedures used to isolate the RAS function from other functions in the device.

d. Describe the procedures used when each multifunction device is removed from service and whether coordination with other protection schemes is required.

e. Describe how each multifunction device is tested, both for commissioning and during periodic maintenance testing, with regard to each function of the device.

f. Describe how overall periodic RAS functional and throughput tests are performed if multifunction devices are used for both local protection and RAS.

g. Describe how upgrades to the multifunction device, such as firmware upgrades, are accomplished. How is the RAS function taken into consideration?

Other devices that are usually not considered multifunction devices such as auxiliary relays, control switches, and instrument transformers may serve multiple purposes such as protection and RAS. Similar concerns apply for these applications as noted above.

4. Documentation describing the System performance resulting from a single component failure in the RAS, except for limited impact RAS, when the RAS is intended to operate. A single component failure in a RAS not determined to be limited impact must not prevent the BES from meeting the same performance requirements (defined in Reliability Standard TPL-001-4 or its successor) as those required for the events and conditions for which the RAS is designed. The documentation should describe or illustrate how the design achieves this objective. [Reference NERC Reliability Standard PRC-012, R1.3]

   RAS automatic arming, if applicable, is vital to RAS and System performance and is therefore included in this requirement.

   Acceptable methods to achieve this objective include, but are not limited to the following:

   a. Providing redundancy of RAS components. Typical examples are listed below:

      i. Protective or auxiliary relays used by the RAS.

ii. Communications systems necessary for correct operation of the RAS.

iii. Sensing devices used to measure electrical or other quantities used by the RAS.

iv. Station dc supply associated with RAS functions.

v. Control circuitry associated with RAS functions through the trip coil(s) of the circuit breakers or other interrupting devices.

vi. Logic processing devices that accept System inputs from RAS components or other sources, make decisions based on those inputs, or initiate output signals to take remedial actions.

b. Arming more load or generation than necessary such that failure of the RAS to drop a portion of load or generation due to that single component failure will still result in satisfactory System performance, as long as tripping the total armed amount of load or generation does not cause other adverse impacts to reliability.

c. Using alternative automatic actions to back up failures of single RAS components.

d. Manual backup operations, using planned System adjustments such as Transmission configuration changes and re-dispatch of generation, if such adjustments are executable within the time duration applicable to the Facility Ratings.

5. Documentation describing the functional testing process.

IV. RAS Retirement

The following checklist identifies important RAS information for each existing RAS to be retired that the RAS-entity shall document and provide to the Reliability Coordinator for review pursuant to Requirement R1.

1. Information necessary to ensure that the Reliability Coordinator is able to understand the physical and electrical location of the RAS and related facilities.

2. A summary of technical studies and technical justifications, if applicable, upon which the decision to retire the RAS is based.

3. Anticipated date of RAS retirement.

While the documentation necessary to evaluate RAS removals is not as extensive as for new or functionally modified RAS, it is still vital that, when the RAS is no longer available, System performance will still meet the appropriate (usually TPL) requirements for the Contingencies or System conditions that the RAS had been installed to remediate.

Technical Justification for Attachment 2 Content

Reliability Coordinator RAS Review Checklist

Attachment 2 is a checklist provided to facilitate consistent reviews continent-wide for new or functionally modified RAS prior to the RAS installation. The checklist is meant to assist the RC in identifying reliability-related considerations relevant to various aspects of RAS design and implementation.

Technical Justifications for Attachment 3 Content

Database Information

Attachment 3 contains the minimum information that the RC must consolidate into its database for each RAS in its area.

1. RAS name.
   - The name used to identify the RAS.
2. Each RAS-entity and contact information.
   - A reliable phone number or email address should be included to contact each RAS-entity if more information is needed.
3. Expected or actual in-service date; most recent (Requirement R3) RC-approval date; most recent five full calendar year (Requirement R4) evaluation date; and, date of retirement, if applicable.
   - Specify each applicable date.
4. System performance issue or reason for installing the RAS (e.g., thermal overload, angular instability, poor oscillation damping, voltage instability, under-/over-voltage, slow voltage recovery).
   - A short description of the reason for installing the RAS is sufficient, as long as the main System issues addressed by the RAS can be identified by someone with a reliability need.
5. Description of the Contingencies or System conditions for which the RAS was designed (initiating conditions).
   - A high level summary of the conditions/Contingencies is expected. Not all combinations of conditions are required to be listed.
6. Corrective action taken by the RAS.
   - A short description of the actions should be given. For schemes shedding load or generation, the maximum amount of megawatts should be included.

7. Identification of limited impact[10] RAS.
    - Specify whether or not the RAS is designated as limited impact.
8. Any additional explanation relevant to high-level understanding of the RAS.
    - If deemed necessary, any additional information can be included in this section, but is not mandatory.

[10] A RAS designated as limited impact cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations.

Rationale

Rationale for Requirement R1: Each Remedial Action Scheme (RAS) is unique and its action(s) can have a significant impact on the reliability and integrity of the Bulk Electric System (BES). Therefore, a review of a proposed new RAS or an existing RAS proposed for functional modification or retirement; i.e., removal from service must be completed prior to implementation or retirement.

Functional modifications consist of any of the following:

- Changes to System conditions or Contingencies monitored by the RAS
- Changes to the actions the RAS is designed to initiate
- Changes to RAS hardware beyond in-kind replacement; i.e., match the original functionality of existing components
- Changes to RAS logic beyond correcting existing errors
- Changes to redundancy levels; i.e., addition or removal

To facilitate a review that promotes reliability, the RAS-entity must provide the reviewer with sufficient details of the RAS design, function, and operation. This data and supporting documentation are identified in Attachment 1 of this standard, and Requirement R1 mandates that the RAS-entity provide them to the reviewing Reliability Coordinator (RC). The RC (reviewing RC) that coordinates the area where the RAS is located is responsible for the review. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate and submit a single, coordinated Attachment 1 to the reviewing RC. In cases where a RAS crosses RC Area boundaries, each affected RC is responsible for conducting either individual reviews or participating in a coordinated review.

Rationale for Requirement R2: The RC is the functional entity best suited to perform the RAS review because it has the widest area operational and reliability perspective of all functional entities and an awareness of reliability issues in any neighboring RC Area. This Wide Area purview facilitates the evaluation of interactions among separate RAS as well as interactions among RAS and other protection and control systems. Review by the RC also minimizes the possibility of a conflict of interest that could exist because of business relationships among the RAS-entity, Planning Coordinator (PC), Transmission Planner (TP), or other entities that are likely to be involved in the planning or implementation of a RAS. The RC is not expected to possess more information or ability than anticipated by their functional registration as designated by NERC. The RC may request assistance to perform RAS reviews from other parties such as the PC or regional technical groups; however, the RC will retain the responsibility for compliance with this requirement.

Attachment 2 of this standard is a checklist the RC can use to identify design and implementation aspects of RAS and facilitate consistent reviews for each submitted RAS. The time frame of four full calendar months is consistent with current utility and regional practice;

however, flexibility is provided by allowing the RC(s) and RAS-entity(ies) to negotiate a mutually agreed upon schedule for the review.

Note: An RC may need to include this task in its reliability plan(s) for the NERC Regions(s) in which it is located.

Rationale for Requirement R3: The RC review is intended to identify reliability issues that must be resolved before the RAS can be put in service. Examples of reliability issues include a lack of dependability, security, or coordination.

A specific time period for the RAS-entity to respond to the reviewing RC following identification of any reliability issue(s) is not necessary because the RAS-entity wants to expedite the timely approval and subsequent implementation of the RAS.

A specific time period for the RC to respond to the RAS-entity following the RAS review is also not necessary because the RC will be aware of (1) any reliability issues associated with the RAS not being in service and (2) the RAS-entity's schedule to implement the RAS to address those reliability issues. Since the RC is the ultimate arbiter of BES operating reliability, resolving reliability issues is a priority for the RC and serves as an incentive to expeditiously respond to the RAS-entity.

Rationale for Requirement R4: Requirement R4 mandates that an evaluation of each RAS be performed at least once every five full calendar years. The purpose of the periodic RAS evaluation is to verify the continued effectiveness and coordination of the RAS, as well as to verify that, if a RAS single component malfunction or single component failure were to occur, the requirements for BES performance would continue to be satisfied. A periodic evaluation is required because changes in System topology or operating conditions may change the effectiveness of a RAS or the way it impacts the BES.

RAS are unique and customized assemblages of protection and control equipment that vary in complexity and impact on the reliability of the BES. In recognition of these differences, RAS can be designated by the reviewing RC(s) as limited impact. A limited impact RAS cannot, by inadvertent operation or failure to operate, cause or contribute to BES Cascading, uncontrolled separation, angular instability, voltage instability, voltage collapse, or unacceptably damped oscillations. The "BES" qualifier in the preceding statement modifies all of the conditions that follow it. Limited impact RAS are not subject to the RAS single component malfunction and failure tests of Parts 4.1.4 and 4.1.5, respectively. Requiring a limited impact RAS to meet these tests would add complexity to the design with minimal benefit to BES reliability. See the Supplemental Material for more on the limited impact designation.

The standard recognizes the Local Area Protection Scheme (LAPS) classification in WECC (Western Electricity Coordinating Council) and the Type III classification in NPCC (Northeast Power Coordinating Council) as initially appropriate for limited impact designation. A RAS implemented prior to the effective date of PRC-012-2 that has been through the regional

review processes of WECC or NPCC and is classified as either a Local Area Protection Scheme (LAPS) in WECC or a Type III in NPCC is recognized as a limited impact RAS upon the effective date of PRC-012-2 for the purposes of this standard and is subject to all applicable requirements.

For existing RAS, the initial performance of Requirement R4 must be completed within five full calendar years of the effective date of PRC-012-2. For new or functionally modified RAS, the initial performance of the requirement must be completed within five full calendar years of the RAS approval date by the reviewing RC(s). Five full calendar years was selected as the maximum time frame between evaluations based on the time frames for similar requirements in Reliability Standards PRC-006, PRC-010, and PRC-014. The RAS evaluation can be performed sooner if it is determined that material changes to System topology or System operating conditions could potentially impact the effectiveness or coordination of the RAS. System changes also have the potential to alter the reliability impact of limited impact RAS on the BES. Requirement 4, Part 4.1.3 explicitly requires the periodic evaluation of limited impact RAS to verify the limited impact designation remains applicable; the PC can use its discretion as to how this evaluation is performed. The periodic RAS evaluation will typically lead to one of the following outcomes: 1) affirmation that the existing RAS is effective; 2) identification of changes needed to the existing RAS; or, 3) justification for RAS retirement.

The items required to be addressed in the evaluations (Requirement R4, Parts 4.1.1 through 4.1.5) are planning analyses that may involve modeling of the interconnected transmission system to assess BES performance. The Planning Coordinator (PC) is the functional entity best suited to perform this evaluation because they have a wide area planning perspective. To promote reliability, the PC is required to provide the results of the evaluation to each impacted Transmission Planner and Planning Coordinator, in addition to each reviewing RC and RAS-entity. In cases where a RAS crosses PC boundaries, each affected PC is responsible for conducting either individual evaluations or participating in a coordinated evaluation.

The previous version of this standard (PRC-012-1 Requirement 1, R1.4) states "… the inadvertent operation of a RAS shall meet the same performance requirement (TPL-001-0, TPL-002-0, and TPL-003-0) as that required of the Contingency for which it was designed, and not exceed TPL-003-0." Requirement R4 clarifies that the inadvertent operation to be considered would only be that caused by the malfunction of a single RAS component. This allows security features to be designed into the RAS such that inadvertent operation due to a single component malfunction is prevented. Otherwise, consistent with PRC-012-1 Requirement 1, R1.4, the RAS should be designed so that its whole or partial inadvertent operation due to a single component malfunction satisfies the System performance requirements for the same Contingency for which the RAS was designed.

If the RAS was installed for an extreme event in TPL-001-4 or for some other Contingency or System condition not defined in TPL-001-4 (therefore without performance requirements), its inadvertent operation still must meet some minimum System performance requirements. However, instead of referring to the TPL-001-4, Requirement R4 lists the System performance

requirements that the inadvertent operation must satisfy. The performance requirements listed (Parts 4.1.4.1 – 4.1.4.5) are the ones that are common to all planning events P0-P7 listed in TPL-001-4.

Rationale for Requirement R5: The correct operation of a RAS is important for maintaining the reliability and integrity of the BES. Any incorrect operation of a RAS indicates that the RAS effectiveness and/or coordination has been compromised. Therefore, all operations of a RAS and failures of a RAS to operate when expected must be analyzed to verify that the RAS operation was consistent with its intended functionality and design.

A RAS operational performance analysis is intended to: 1) verify RAS operation was consistent with the implemented design; or 2) identify RAS performance deficiencies that manifested in the incorrect RAS operation or failure of RAS to operate when expected.

The 120 full calendar day time frame for the completion of RAS operational performance analysis aligns with the time frame established in Requirement R1 from PRC-004-4 regarding the investigation of a Protection System Misoperation. To promote reliability, each RAS-entity is required to provide the results of RAS operational performance analyses that identified any deficiencies to its reviewing RC(s).

RAS-entities may need to collaborate with their associated Transmission Planner to comprehensively analyze RAS operational performance. This is because a RAS operational performance analysis involves verifying that the RAS operation was triggered correctly (Part 5.1.1), responded as designed (Part 5.1.2), and that the resulting BES response (Parts 5.1.3 and 5.1.4) was consistent with the intended functionality and design of the RAS. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to conduct and submit a single, coordinated operational performance analysis.

Rationale for Requirement R6: Deficiencies identified in the periodic RAS evaluation conducted by the PC pursuant to Requirement R4, in the operational performance analysis conducted by the RAS-entity pursuant to Requirement R5, or in the functional test performed by the RAS-entity pursuant to Requirement R8, potentially pose a reliability risk to the BES. To mitigate these potential reliability risks, Requirement R6 mandates that each RAS-entity develop a Corrective Action Plan (CAP) to address the identified deficiency. The CAP contains the mitigation actions and associated timetable necessary to remedy the specific deficiency. The RAS-entity may request assistance with CAP development from other parties such as its Transmission Planner or Planning Coordinator; however, the RAS-entity has the responsibility for compliance with this requirement.

If the CAP requires that a functional change be made to a RAS, the RAS-entity will need to submit information identified in Attachment 1 to the reviewing RC(s) prior to placing RAS modifications in service per Requirement R1.

Depending on the complexity of the identified deficiency(ies), development of a CAP may require studies, and other engineering or consulting work. A maximum time frame of six full calendar months is specified for RAS-entity collaboration on the CAP development. Ideally, when there is more than one RAS-entity for a RAS, the RAS-entities would collaborate to develop and submit a single, coordinated CAP.

Rationale for Requirement R7: Requirement R7 mandates each RAS-entity implement a CAP (developed in Requirement R6) that mitigates the deficiencies identified in Requirements R4, R5, or R8. By definition, a CAP is: "A list of actions and an associated timetable for implementation to remedy a specific problem." The implementation of a properly developed CAP ensures that RAS deficiencies are mitigated in a timely manner. Each reviewing Reliability Coordinator must be notified if CAP actions or timetables change, and when the CAP is completed.

Rationale for Requirement R8: Due to the wide variety of RAS designs and implementations, and the potential for impacting BES reliability, it is important that periodic functional testing of a RAS be performed. A functional test provides an overall confirmation of the RAS to operate as designed and verifies the proper operation of the non-Protection System (control) components of a RAS that are not addressed in PRC-005. Protection System components that are part of a RAS are maintained in accordance with PRC-005.

The six or twelve full calendar year test interval, which begins on the effective date of the standard pursuant to the PRC-012-2 implementation plan, is a balance between the resources required to perform the testing and the potential reliability impacts to the BES created by undiscovered latent failures that could cause an incorrect operation of the RAS. Extending to longer intervals increases the reliability risk to the BES posed by an undiscovered latent failure that could cause an incorrect operation or failure of the RAS. The RAS-entity is in the best position to determine the testing procedure and schedule due to its overall knowledge of the RAS design, installation, and functionality. Functional testing may be accomplished with end-to-end testing or a segmented approach. For segmented testing, each segment of a RAS must be tested. Overlapping segments can be tested individually negating the need for complex maintenance schedules and outages.

The maximum allowable interval between functional tests is six full calendar years for RAS that are not designated as limited impact RAS and twelve full calendar years for RAS that are designated as limited impact RAS. The interval between tests begins on the date of the most recent successful test for each individual segment or end-to-end test. A successful test of one segment only resets the test interval clock for that segment. A correct operation of a RAS qualifies as a functional test for those RAS segments which operate (documentation for compliance with Requirement R5 Part 5.1). If an event causes a partial operation of a RAS, the segments without an operation will require a separate functional test within the maximum interval with the starting date determined by the previous successful test of the segments that did not operate.

Supplemental Material

Rationale for Requirement R9: The RAS database is a comprehensive record of all RAS existing in a Reliability Coordinator Area. The database enables the RC to provide other entities high-level information on existing RAS that could potentially impact the operational and/or planning activities of that entity. Attachment 3 lists the minimum information required for the RAS database, which includes a summary of the RAS initiating conditions, corrective actions, and System issues being mitigated. This information allows an entity to evaluate the reliability need for requesting more detailed information from the RAS-entities identified in the database contact information. The RC is the appropriate entity to maintain the database because the RC receives the required database information when a new or modified RAS is submitted for review. The twelve full calendar month time frame is aligned with industry practice and allows sufficient time for the RC to collect the appropriate information from RAS-entities and update the RAS database.

A. Introduction

1. **Title:** **Transmission Operations**

2. **Number:** TOP-001-4

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. Each Transmission Operator shall have data exchange capabilities with the entities it has identified it needs data from in order to perform its Operational Planning Analyses. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M19. Each Transmission Operator shall have, and provide upon request, evidence that could include, but is not limited to, operator logs, system specifications, system diagrams, or other evidence that it has data exchange capabilities with the entities it has identified it needs data from in order to perform its Operational Planning Analyses.

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. Each Balancing Authority shall have data exchange capabilities with the entities it has identified it needs data from in order to develop its Operating Plan for next-day operations. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M22. Each Balancing Authority shall have, and provide upon request, evidence that could include, but is not limited to, operator logs, system specifications, system diagrams, or

other evidence that it has data exchange capabilities with the entities it has identified it needs data from in order to develop its Operating Plan for next-day operations.

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 R19, and Measure M15 through M19 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 R22 and Measure M22 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 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 comply with an Operating Instruction issued by its Transmission Operator.

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

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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 equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	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 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	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 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, or associated communication channels between the affected entities.	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. 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	The Transmission Operator did not monitor, obtain, or utilize two of the items required or	The Transmission Operator did not monitor, obtain, or utilize three of the items required or	The Transmission Operator did not monitor, obtain, or utilize four or more of the items

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	required or identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	identified as necessary by the Transmission Operator and listed in Requirement R10, Part 10.1 through 10.6.	required or identified as necessary by the Transmission Operator and listed in Requirement R10 Part 10.1 through 10.6.
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.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R14.	N/A	N/A	N/A	The Transmission Operator did not initiate its Operating 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 authority to approve planned outages and maintenance of its telemetering and control

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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	The Transmission Operator did not have data exchange capabilities for performing its Operational Planning Analyses with one identified entity, or 5% or less of the applicable entities, whichever is greater.	The Transmission Operator did not have data exchange capabilities for performing its Operational Planning Analyses with two identified entities, or more than 5% or less than or equal to 10% of the applicable entities, whichever is greater.	The Transmission Operator did not have data exchange capabilities for performing its Operational Planning Analyses with three identified entities, or more than 10% or less than or equal to 15% of the applicable entities, whichever is greater.	The Transmission Operator did not have data exchange capabilities for performing its Operational Planning Analyses with four or more identified entities or greater than 15% of the applicable entities, whichever is greater.
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 diversely routed data exchange infrastructure within the Transmission Operator's primary Control	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
			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 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.	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 redundant functionality in more than 4 hours and less than or equal to 6 hours.	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 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, 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 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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				functionality.
R22	The Balancing Authority did not have data exchange capabilities for developing its Operating Plan with one identified entity, or 5% or less of the applicable entities, whichever is greater.	The Balancing Authority did not have data exchange capabilities for developing its Operating Plan with two identified entities, or more than 5% or less than or equal to 10% of the applicable entities, whichever is greater.	The Balancing Authority did not have data exchange capabilities for developing its Operating Plan with three identified entities, or more than 10% or less than or equal to 15% of the applicable entities, whichever is greater.	The Balancing Authority did not have data exchange capabilities for developing its Operating Plan with four or more identified entities or greater than 15% of the applicable entities, whichever is greater.
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 Authority's primary Control Center, as specified in the Requirement.	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.
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	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	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;	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;

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	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 2 hours and less than or equal to 4 hours.	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 4 hours and less than or equal to 6 hours.	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 6 hours and less than or equal to 8 hours.	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 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 Implementation Plan and other project documents can be found on the project page.

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	

Guidelines and Technical Basis

None

Rationale

During development of TOP-001-4, text boxes are embedded within the standard to explain the rationale for various parts of the standard. Upon Board adoption of TOP-001-4, the text from the rationale text boxes will be moved to this section.

Rationale text from the development of TOP-001-3 in Project 2014-03 follows. Additional information can be found on the Project 2014-03 project page.

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):

Added for consistency with proposed IRO-002-4, Requirement R1. Data exchange capabilities are required to support the data specification concept in proposed TOP-003-3.

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.

Supplemental Material

Rationale for Requirements R22 and R23:

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:** **Real-time Reliability Monitoring and Analysis Capabilities**

2. **Number:** **TOP-010-1(i)**

3. **Purpose:** Establish requirements for Real-time monitoring and analysis capabilities to support reliable System operations.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Transmission Operators

   4.1.2. Balancing Authorities

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

B. Requirements and Measures

R1. Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

1.1. Criteria for evaluating the quality of Real-time data;

1.2. Provisions to indicate the quality of Real-time data to the System Operator; and

1.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.

M1. Each Transmission Operator shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R1; and 2) evidence the Transmission Operator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R2. Each Balancing Authority shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: High] [Time Horizon: Real-time Operations]*

2.1. Criteria for evaluating the quality of Real-time data;

2.2. Provisions to indicate the quality of Real-time data to the System Operator; and

2.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects its analysis functions.

M2. Each Balancing Authority shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R2; and 2) evidence the Balancing Authority implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R3. Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments. The Operating Process or Operating Procedure shall include: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

3.1. Criteria for evaluating the quality of analysis used in its Real-time Assessments;

3.2. Provisions to indicate the quality of analysis used in its Real-time Assessments; and

3.3. Actions to address analysis quality issues affecting its Real-time Assessments.

M3. Each Transmission Operator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments as specified in Requirement R3. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R3; and 2) evidence the Transmission Operator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.

R4. Each Transmission Operator and Balancing Authority shall have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. Each Transmission Operator and Balancing Authority shall have evidence of an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred. This evidence could include, but is not limited to, operator logs, computer printouts, system specifications, or other evidence.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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 it was compliant for the full-time period since the last audit.

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

The applicable entity shall retain evidence of compliance for Requirements R1, R2, and R4, and Measures M1, M2, and M4 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Transmission Operator shall retain evidence of compliance for Requirement R3 and Measure M3 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If an applicable entity is found non-compliant it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include one of the elements listed in Part 1.1 through Part 1.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include two of the elements listed in Part 1.1 through Part 1.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments did not include any of the elements listed in Part 1.1 through Part 1.3; OR The Transmission Operator did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments.
R2.	N/A	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the	The Balancing Authority's Operating Process or Operating Procedure to address the quality of the

		Real-time data necessary to perform its analysis functions and Real-time monitoring did not include one of the elements listed in Part 2.1 through Part 2.3.	Real-time data necessary to perform its analysis functions and Real-time monitoring did not include two of the elements listed in Part 2.1 through Part 2.3.	Real-time data necessary to perform its analysis functions and Real-time monitoring did not include any of the elements listed in Part 2.1 through Part 2.3; OR The Balancing Authority did not implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring.
R3.	N/A	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include one of the elements listed in Part 3.1 through Part 3.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include two of the elements listed in Part 3.1 through Part 3.3.	The Transmission Operator's Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments did not include any of the elements listed in Part 3.1 through Part 3.3; OR The Transmission Operator did not implement an Operating Process or Operating Procedure to address the quality of

				analysis used in its Real-time Assessments.
R4.	N/A	N/A	The responsible entity has an alarm process monitor but the alarm process monitor did not provide notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor occurred.	The responsible entity does not have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan

Version History

Version	Date	Action	Change Tracking
1	October 30, 2015	New standard developed in Project 2009-02 to respond to recommendations in Real-time Best Practices Task Force Report and FERC directives.	N/A
1	May 5, 2016	Adopted by the Board of Trustees	New
1	September 22, 2016	FERC Order issued approving TOP-010-1. Docket No. RD16-6-000	
1(i)	September 22, 2016	FERC directive to change Requirement 1 and Requirement 2 from ‘medium’ to ‘high’. Docket No.	Revised

		RD16-6-000	
1(i)	November 2, 2016	Adopted by the Board of Trustees	New
1(i)	December 14, 2016	FERC letter Order approving revisions to the VRF for R1 and R2 from 'medium' to 'high'. Docket No. RD16-6-001.	

Guidelines and Technical Basis

Real-time monitoring, or *monitoring* the Bulk Electric System (BES) in Real-time, is a primary function of Reliability Coordinators (RCs), Transmission Operators (TOPs), and Balancing Authorities (BAs) as required by TOP and IRO Reliability Standards. As used in TOP and IRO Reliability Standards, monitoring involves observing operating status and operating values in Real-time for awareness of system conditions. Real-time monitoring may include the following activities performed in Real-time:

- Acquisition of operating data;
- Display of operating data as needed for visualization of system conditions;
- Audible or visual alerting when warranted by system conditions; and
- Audible or visual alerting when monitoring and analysis capabilities degrade or become unavailable.

Requirement R1

The TOP uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform monitoring and Real-time Assessments appear in other Reliability Standards.

The TOP's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R1 Part 1.1. The criteria support identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 specifies the TOP shall include actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments. Requirement R1 Part 1.3 is focused on addressing data point quality issues affecting Real-time Assessments. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R1 Part 1.3.

The TOP's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the TOP to meet its obligations for performing the Real-time Assessment. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the TOP;
- Following processes established for resolving data conflicts as specified in TOP-003-3, or other applicable Reliability Standards;
- Taking corrective actions on the TOP's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the TOP's Real-time Assessment; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the quality of the Real-time Assessment so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R2

The BA uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The BA's Operating Process or Operating Procedure must contain criteria for evaluating the quality of Real-time data as specified in proposed TOP-010-1 Requirement R2 Part 2.1. The criteria supports identification of applicable data quality issues, which may include:

- Data outside of a prescribed data range;
- Analog data not updated within a predetermined time period;
- Data entered manually to override telemetered information; or
- Data otherwise identified as invalid or suspect.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 specifies the BA shall include in its Operating Process or Operating Procedure actions to address Real-time data quality issues when data quality affects its analysis functions. Requirement R2 Part 2.3 is focused on addressing data point quality issues affecting analysis functions. Other data quality issues of a lower priority are addressed according to an entity's operating practices and are not covered under Requirement R2 Part 2.3.

The BA's actions to address data quality issues are steps within existing authorities and capabilities that provide awareness and enable the BA to meet its obligations for performing its analysis functions. Examples of actions to address data quality issues include, but are not limited to, the following:

- Notifying entities that provide Real-time data to the BA;

- Following processes established for resolving data conflicts as specified in TOP-003-3 or other applicable Reliability Standards;
- Taking corrective actions on the BA's own data;
- Changing data sources or other inputs so that the data quality issue no longer affects the BA's analysis functions; and
- Inputting data manually and updating as necessary.

The Operating Process or Operating Procedure must clearly identify to operating personnel how to determine the data that affects the analysis quality so that effective actions can be taken to address data quality issues in an appropriate timeframe.

Requirement R3

Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments may include, as applicable, state estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

Examples of the types of criteria used to evaluate the quality of analysis used in Real-time Assessments may include solution tolerances, mismatches with Real-time data, convergences, etc.

The Operating Process or Operating Procedure must describe how the quality of analysis results used in Real-time Assessment will be shown to operating personnel.

Requirement R4

Requirement R4 addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

An alarm process monitor could be an application within a Real-time monitoring system or it could be a separate system. 'Heartbeat' or 'watchdog' monitors are examples of an alarm process monitor. An alarm process monitor should be designed and implemented such that a stall of the Real-time monitoring alarm processor does not cause a failure of the alarm process monitor.

Rationale

Rationale for Requirement R1: The Transmission Operator (TOP) uses a set of Real-time data identified in TOP-003-3 Requirement R1 to perform its Real-time monitoring and Real-time Assessments. Functional requirements to perform Real-time monitoring and Real-time Assessments appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R1 Part 1.3 of this standard specifies the TOP shall include actions to address Real-time data quality issues affecting its Real-time Assessments in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process used to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2, provided that this process addresses Real-time data quality issues.

The revision in Part 1.3 to address Real-time data quality issues *when data quality affects Real-time Assessments* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R2: The Balancing Authority (BA) uses a set of Real-time data identified in TOP-003-3 Requirement R2 to perform its analysis functions and Real-time monitoring. Requirements to perform monitoring appear in other Reliability Standards.

The Operating Process or Operating Procedure must include provisions for indicating the quality of Real-time data to operating personnel. Descriptions of quality indicators such as display color codes, data quality flags, or other such indicators as found in Real-time monitoring specifications could be used.

Requirement R2 Part 2.3 of this standard specifies the BA shall include actions to address Real-time data quality issues affecting its analysis functions in its Operating Process or Operating Procedure. Examples of actions to address Real-time data quality issues are provided in the Guidelines and Technical Basis section. These actions could be the same as the process to resolve data conflicts required by TOP-003-3 Requirement R5 Part 5.2 provided that this process addresses Real-time data quality issues.

The revision in Part 2.3 to address Real-time data quality issues *when data quality affects its analysis functions* clarifies the scope of data points that must be covered by the Operating Process or Operating Procedure.

Rationale for Requirement R3: Requirement R3 ensures TOPs have procedures to address issues related to the quality of the analysis results used for Real-time Assessments. Requirements to perform Real-time Assessments appear in other Reliability Standards. Examples of the types of analysis used in Real-time Assessments include, as applicable, state

estimation, Real-time Contingency analysis, Stability analysis or other studies used for Real-time Assessments.

The Operating Process or Operating Procedure must include provisions for how the quality of analysis results used in Real-time Assessment will be shown to operating personnel. Operating personnel includes System Operators and staff responsible for supporting Real-time operations.

Rationale for Requirement R4: The requirement addresses recommendation S7 of the Real-time Best Practices Task Force report concerning operator awareness of alarm availability.

The requirement in Draft Two of the proposed standard has been revised for clarity by removing the term *independent*. The alarm process monitor must be able to provide notification of failure of the Real-time monitoring alarm processor. This capability could be provided by an application within a Real-time monitoring system or by a separate component used by the System Operator. The alarm process monitor must not fail with a simultaneous failure of the Real-time monitoring alarm processor.

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-4.2

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in Real-time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators

   4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. **Effective Date*:**

   5.1. The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operations planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled.

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as necessary in Real-time. This may include, but is not limited to, instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

R4. Each Transmission Operator shall specify the criteria that will exempt generators: 1) from following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generator in its area that is exempt: 1) from following a voltage or Reactive Power schedule, 2) from having its

automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band). For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) within 30 days of receiving a request by a Generator Operator.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The British Columbia Utilities Commission

Evidence Retention:

The following evidence retention periods identify the period of time a registered entity is required to retain specific evidence to demonstrate compliance. For instances in which the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask the registered entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Operator shall retain evidence for Measures M1 through M6 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.2. Compliance Monitoring and Assessment Processes:

“Compliance Monitoring and Assessment Processes” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.3. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	N/A	N/A	N/A	The Transmission Operator does not specify a system voltage schedule (which is either a range or a target value with an associated tolerance band).
R2	**Real-time Operations, Same-day Operations, and Operations Planning**	**High**	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	**Real-time Operations, Same-day Operations, and Operations Planning**	**High**	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Planning**	**Lower**	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification to the Generator Operator.	The Transmission Operator does not have exemption criteria.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	**Operations Planning**	**Medium**	N/A	The Transmission Operator does not provide the criteria for voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) after 30 days of a request.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to all Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to any Generator Operators. Or The Transmission Operator does not provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	The Transmission Operator does not provide either the technical justification or timeframe for changing generator step-up tap settings.	N/A	N/A	The Transmission Operator does not provide the technical justification and the timeframe for changing generator step-up tap settings.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R4 and R5. Please note that Requirement R4 is deleted and R5 is replaced with the following requirements.

Requirements

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

E.A.15 Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

E.A.16 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.17 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.18 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the automatic voltage regulators (AVR) to manage Mvar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.18.1. Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.18.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures[1]

M.E.A.13 Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

M.E.A.14 The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

M.E.A.15 Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

M.E.A.16 The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.E.A.17 The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.E.A.18 If the Generator Operator uses outside control loops to manage Mvar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence.

[1] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

Violation Severity Levels

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.13	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to at least one generation resource but less than or equal to 5% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 5% but less than or equal to 10% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 10% but less than or equal to 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.
E.A.14	The Transmission Operator did not provide a voltage schedule reference point for at least one but less than or equal to 5% of the generation resources in the Transmission Operator area.	The Transmission Operator did not provide a voltage schedule reference point for more than 5% but less than or equal to 10% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not a voltage schedule reference point for more than 10% but less than or equal to 15% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not provide a voltage schedule reference point for more than 15% of the generation resources in the Transmission Operator Area.
E.A.15	The Generator Operator failed to convert at least one voltage schedule in Requirement E.A.13 into the voltage set point for the AVR for less than 25% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 25% or more but less than 50% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 50% or more but less than 75% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 75% or more of the voltage schedules.

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.16	The Generator Operator provided its voltage set point conversion methodology greater than 30 days but less than or equal to 60 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Transmission Operator.	The Generator Operator did not provide its voltage set point conversion methodology within 120 days of a request by the Transmission Operator.
E.A.17	The Transmission Operator provided its data to support development of the voltage set point conversion methodology than 30 days but less than or equal to 60 days of a request by the Generator Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Generator. Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Generator. Operator.	The Transmission Operator did not provide its data to support development of the voltage set point conversion methodology within 120 days of a request by the Generator Operator.
E.A.18	N/A	The Generator Operator did not meet the control loop specifications in EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in EA18.1 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in EA18.1 through EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.

E. Interpretations

None

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	June 18, 2007	FERC approved Version 1 of the standard.	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	August 5, 2010	Adopted by NERC Board of Trustees; Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised
2	January, 10 2011	FERC issued letter order approving the addition of LSEs and Controllable Load to the standard.	Revised
3	May 9, 2012	Adopted by NERC Board of Trustees; Modified to add a WECC region variance	Revised
3	June 20, 2013	FERC issued order approving VAR-001-3	Revised
3	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	Revised
4	February 6, 2014	Adopted by NERC Board of Trustees	Revised
4	August 1, 2014	FERC issued letter order issued approving VAR-001-4	
4.1	August 25, 2015	Added “or” to Requirement R5, 5.3 to read: schedules or Reactive Power	Errata
4.1	November 13, 2015	FERC Letter Order approved errata to VAR-001-4.1. Docket RD15-6-000	Errata
4.2	June 14, 2017	Project 2016-EPR-02 errata recommendations	Errata
4.2	August 10, 2017	Adopted by NERC Board of Trustees	Errata
4.2	September 26, 2017	FERC Letter Order issued approving VAR-001-4.2 Docket No. RD17-7-000.	

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

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:

Paragraph 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, however, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (SOLs) and reliability margins are established. The NERC Glossary definition of SOLs includes both: 1) voltage stability ratings (Applicable pre- and post-Contingency Voltage Stability) and 2*)* System Voltage Limits (Applicable pre- and post-Contingency voltage limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

Rationale for R2:

Paragraph 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not explicitly require the periodic voltage stability analysis because such analysis would be performed pursuant to the SOL methodology developed under the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits (IROL). The VAR standard drafting team (SDT) and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at Paragraph 1879.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific

area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

A. Introduction

1. **Title:** **Generator Operation for Maintaining Network Voltage Schedules**

2. **Number:** **VAR-002-4.1**

3. **Purpose:** To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Generator Operator

   4.2. Generator Owner

5. **Effective Dates***

   See Implementation Plan.

B. Requirements and Measures

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.

[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.

Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For Part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For Part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For Part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, Reactive Power capability may change based on stability considerations.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- Reporting of status or capability changes as stated in Requirement R4 is not applicable to the individual generating units of dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition.

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up and auxiliary transformers[5] with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up and auxiliary transformers as required in Requirement R5, Part 5.1.1 through Part 5.1.3 within 30 calendar days.

[5] For dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies only to those transformers that have at least one winding at a voltage of 100 kV or above.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6, Part 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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 Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage control mode or in a different control mode as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Real-time Operations**	**Medium**	N/A	N/A	The Generator Operator did not have a conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator did not maintain the voltage or Reactive Power schedule as instructed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any explanation.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of the status change.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of becoming aware of the capability change.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator Owner failed to provide its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.	The Generator Owner failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.

VAR-002-4.1 — Generator Operation for Maintaining Network Voltage Schedules

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR The Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it could not comply with the Transmission Operator specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised
3	5/5/2014	Revised under Project 2013-04 to address outstanding Order 693 directives.	Revised
3	5/7/2014	Adopted by NERC Board of Trustees	
3	8/1/2014	Approved by FERC in docket RD14-11-000	
4	8/27/2014	Revised under Project 2014-01 to clarify applicability of Requirements to BES dispersed power producing	Revised

		resources.	
4	11/13/2014	Adopted by NERC Board of Trustees	
4	5/29/2015	FERC Letter Order in Docket No. RD15-3-000 approving VAR-002-4	
4.1	June 14, 2017	Project 2016-EPR-02 errata recommendations	Errata
4.1	August 10, 2017	Adopted by the NERC Board of Trustees	Errata
4.1	September 26, 2017	FERC Letter Order issued approving VAR-002-4.1 RD17-7-000	

Guidelines and Technical Basis

Rationale:

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

Rationale for R1:

This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates its generator(s) to provide voltage support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new Part 2.3 has been added to detail that each GOP may monitor voltage by using its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Notifications of this type of status change provide little to no benefit to reliability. Thirty (30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status change. The requirement has

also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change.

Rationale for R4:

This requirement has been bifurcated from the prior version VAR-002-2b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are not aware of a reactive capability change until it has taken place.

Rationale for Exclusion in R4:

VAR-002 addresses control and management of reactive resources and provides voltage control where it has an impact on the BES. For dispersed power producing resources as identified in Inclusion I4, Requirement R4 should not apply at the individual generator level due to the unique characteristics and small scale of individual dispersed power producing resources. In addition, other standards such as proposed TOP-003 require the Generator Operator to provide Real-time data as directed by the TOP.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected. The prior version of VAR-002-2b, Requirement R4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

Rationale for Exclusion in R5:

The Transmission Operator and Transmission Planner only need to review tap settings, available fixed tap ranges, impedance data and the +/- voltage range with step-change in % for load-tap changing transformers on main generator step-up unit transformers which connect dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition to their transmission system. The dispersed power producing resources individual generator transformers are not intended, designed or installed to improve voltage performance at the point of interconnection. In addition, the dispersed power producing resources individual generator transformers have traditionally been excluded from Requirement R4 and R5 of VAR-002-2b (similar requirements are R5 and R6 for VAR-002-3), as they are not used to improve voltage performance at the point of interconnection.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected.

A. Introduction

1. **Title:** Power System Stabilizer (PSS)

2. **Number:** VAR-501-WECC-3.1

3. **Purpose:** To ensure the Western Interconnection is operated in a coordinated manner under normal and abnormal conditions by establishing the performance criteria for WECC power system stabilizers.

4. **Applicability:**

   4.1 Generator Operator

   4.2 Generator Owner

5. **Facilities:** This standard applies to synchronous generators, connected to the Bulk Electric System, that meet the definition of Commercial Operation.

6. **Effective Date*:** The first day of the first quarter following regulatory approval, except for Requirement R3.

   For units placed in first-time service after regulatory approval, Requirement R3 is effective the first day of the first quarter following final regulatory approval.

   For units placed in service prior to final regulatory approval, Requirement R3 is effective the first day of the first quarter that is five years after regulatory approval.

B. Requirements and Measures

R1. Each Generator Owner shall provide to its Transmission Operator, the Generator Owner's written Operating Procedure or other document(s) describing those known circumstances during which the Generator Owner's PSS will not be providing an active signal to the Automatic Voltage Regulator (AVR), within 180 days of any of the following events: *[Violation Risk Factor: Low] [Time Horizon: Planning Horizon]*

- The effective date of this standard;
- The PSS's Commercial Operation date; or
- Any changes to the PSS operating specifications.

M1. Each Generator Owner will have documented evidence that it provided to its Transmission Operator, within the time allotted as described in the procedures required under Requirement R1, written Operating Procedures or other document(s) describing those known circumstances during which the Generator Owner's PSS will not be providing an active signal to the AVR.

For auditing purposes, because Requirement R1 conditions are intended to be unchanged unless the Transmission Operator is otherwise notified, the Generator Owner only needs to provide the documentation to the Transmission Operator one time, or whenever the operating specifications change.

For auditing purposes, if a PSS is in service but is not providing an active signal to the AVR as described in Requirement R1, the disabled period does not count against the Requirement R2 mandate to be in service except as otherwise allowed.

R2. Each Generator Operator shall have its PSS in service while synchronized, except during any of the following: *[Violation Risk Factor: Medium] [Time Horizon: Operating Assessment]*

- Component failure
- Testing of a Bulk Electric System Element affecting or affected by the PSS
- Maintenance
- As agreed upon by the Generator Operator and the Transmission Operator

A PSS that is out of service for less than 30 minutes does not create a violation of this Requirement, regardless of cause.

M2. Each Generator Operator will have documentation of each claimed exception specified in Requirement R2. Documentation may include, but is not limited to:

- A written explanation covering the bulleted exception that describes the circumstances of the exception as allowed in Requirement R2.
- Documented evidence that the Generator Operator and the Transmission Operator agreed the PSS would not be operating during a specified set of circumstances, where the exception is claimed under the last bullet of Requirement R2.

For auditing purposes, the presumption is that the PSS was in service unless otherwise exempted in Requirement R2. Evidence need only be provided to prove the circumstances during which the PSS was not in service for periods in excess of 30 minutes.

R3. Each Generator Owner shall tune its PSS to meet the following inter-area mode criteria, except as specified in Requirement R3, Part 3.5 below: *[Violation Risk Factor: Medium] [Time Horizon: Operating Assessment]*

3.1. PSS shall be set to provide the measured, simulated, or calculated compensated Vt/Vref frequency response of the excitation system and synchronous machine such that the phase angle will not exceed ± 30 degrees through the frequency range from 0.2 Hertz to the lesser of 1.0 Hertz or the highest frequency at which the phase of the Vt/Vref frequency response does not exceed 90 degrees.

3.2. PSS output limits shall be set to provide at least ±5% of the synchronous machine's nominal terminal voltage.

3.3. PSS gain shall be set to between 1/3 and 1/2 of maximum practical gain.

3.4. PSS washout time constant shall be no greater than 30 seconds.

3.5. Units that have an excitation system or PSS that is incapable of meeting the tuning requirements of Requirement R3 are exempt from Requirement R3 until the voltage regulator is either replaced or retrofitted such that the PSS becomes capable of meeting the tuning requirements.

M3. Each Generator Owner will have documented evidence that its PSS was tuned to meet the specifications of Requirement R3.

If the exception under Requirement R3, Part 3.5, is claimed, the Generator Owner will have documented evidence describing: 1) the conditions that render the PSS incapable of meeting the tuning requirements, and 2) the date the voltage regulator was last replaced or retrofitted.

R4. Each Generator Owner shall install and complete start-up testing of a PSS on its generator within 180 days of either of the following events: *[Violation Risk Factor: Medium] [Time Horizon: Operational Assessment]*

- The Generator Owner connects a generator to the BES, after achieving Commercial Operation, and after the Effective Date of this standard.
- The Generator Owner replaces the voltage regulator on its existing excitation system, after achieving Commercial Operation for its generator that is connected to the BES, and after the Effective Date of this standard.

M4. Each Generator Owner will have evidence that it installed and completed start-up testing of a PSS on its generator within 180 days of either of the conditions described in Requirement R4, and when those conditions occur after the Effective Date of this standard.

For auditing purposes of Requirement R4, bullet one only applies to equipment on its initial (first energization) connection to the BES.

R5. Each Generator Owner shall repair or replace a PSS within 24 months of that PSS becoming incapable of meeting the tuning specifications stated in Requirement R3. *[Violation Risk Factor: Medium] [Time Horizon: Operational Assessment]*

M5. Each Generator Owner will have evidence that it repaired or replaced its PSS within 24 months of that PSS becoming incapable of meeting the tuning specifications of Requirement R3. Evidence may include, but is not limited to, documentation of the date the PSS became incapable of meeting the Requirement R3 tuning specifications, and the date the PSS was returned to service, demonstrating that the span of time between the two events was less than 24 months.

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The British Columbia Utilities Commission.

1.2 Compliance Monitoring and Assessment Processes

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

1.3 Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Generator Operator shall keep evidence for all Requirements of the document for a period of three years plus calendar current.

1.4 Additional Compliance Information

None

D. Regional Differences

None

Table of Compliance Elements

R	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Planning Horizon	Low	NA	NA	NA	The Generator Owner failed to provide its PSS operating specifications to the Transmission Operator as required in Requirement R1.
R2	Operations Assessment	Medium	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 30 minutes but less than 60 minutes.	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 60 minutes but less than 120 minutes.	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 120 minutes but less than 180 minutes.	Each Generator Operator not having its PSS in service while synchronized in accordance with Requirement R2, for more than 180 minutes.
R3	Operations Assessment	Medium	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, two times or fewer during the audit period.	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, three times during the audit period.	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, four times during the audit period.	The Generator Owner's PSS failed to meet any of the required performances in Requirement R3, five times or more during the audit period.

R	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operational Assessment	Medium	NA	NA	NA	The Generator Owner failed to install on its generator a PSS, as required in Requirement R4.
R5	Operational Assessment	Medium	NA	NA	NA	The Generator Owner failed to repair or replace a non-operational PSS as required in Requirement R5.

Version History

Version	Date	Action	Change Tracking
1	April 16, 2008	Permanent Replacement Standard for VAR-STD-002b-1	
1	October 28, 2008	Adopted by NERC Board of Trustees	
1	April 21, 2011	FERC Order issued approving VAR-501-WECC-1 (FERC approval effective June 27, 2011; Effective Date July 1, 2011)	
2	November 13, 2014	Adopted by NERC Board of Trustees	
2	March 3, 2015	FERC letter order approved VAR-501-WECC-2	
3	February 9, 2017	Adopted by NERC Board of Trustees	
3	April 28, 2017	FERC letter order approved VAR-501-WECC-3	
3.1	August 10, 2017	Adopted by the NERC Board of Trustees	Errata
3.1	September 26, 2017	FERC letter order issued approving VAR-501-WECC-3.1	

Guideline and Technical Basis

PSS systems are used to minimize real power oscillations by rapidly adjusting the field of the generator to dampen the low-frequency oscillations.

It is necessary for large numbers of PSS devices to be in operation in the Western Interconnection to provide the required system damping while still allowing for some of these units to be out of service whenever necessary.

Mandate to Install a PSS

Nothing in this Regional Reliability Standard (RSS) should be construed to require installation of a PSS *solely because* a PSS is not currently installed as of the Effective Date of this RRS. Rather, installation is only mandated on the occurrence of either of the triggering events described in Requirement R4, Bullet 1 or Bullet 2, after the Effective Date of the RRS.

It should be noted that a PSS is neither Transmission nor generation.

Requirement R1

Requirement R1 addresses normal operating conditions.

Requirement R1 recognizes that PSS systems have varying states, such as on, off, active, and non-active. As long as the PSS is operating in accordance with the documentation provided to the Transmission Operator, this is not considered a status change for purposes of this standard.

This Requirement eliminates the requirement to count hours as required in the previous version of this standard while also allowing the Generator Owner to create a unit-specific operating plan.

The intent of Requirement R1 is to provide the Transmission Operator, the PSS operating zone in which the PSS is “active” providing damping to the power system. Some PSS may be programmed to become “active” at a specified megawatt loading level and above while others may be programmed to be “active” in a particular band of megawatt loading levels and are “non-active” only when passing through the “rough zone” or some other band. A “rough zone” is a megawatt loading band in which the generator-turbine system could contribute to system instability.

Requirement R2

This Requirement only applies when the PSS is out of service for a period greater than 30 minutes.

Unlike Requirement R1, Requirement R2 addresses exceptions to normal operation.

The intent of Requirement R2 is to remove the previous requirement to log hours for PSS in service. In this standard’s previous version, the logged hours were totaled quarterly to meet the

98% in-service requirement. Instead of documenting the number of hours excluded, this Requirement simplifies the process by allowing the Generator Operator to communicate to the Transmission Operator the circumstances that render the PSS unavailable to the Transmission Operator (such as component failure, maintenance, and testing).

Requirement R3

Nothing in this RSS should be construed to mandate the design criteria for the *equipment* used to produce the tuning output of the PSS. Rather, Requirement R3 is intended to address the design criteria for the *tuning output* of the PSS.

Unlike the language in Requirement R5 that looks *backward* to address units that were once operating but are no longer capable of operating, Requirement R3 looks *forward*, requiring that units be tuned to the specified parameters.

The PSS transfer function should compensate the phase characteristics of the generator, exciter, and power (GEP) system transfer function so the compensated transfer function ((PSS(s) * GEP(s)) has a phase characteristic of ± 30 degrees in the frequency range.

The GEP(s) transfer function is a theoretical transfer function and its phase characteristic cannot be directly measured during field tests (only via simulation). Thus, the Requirement recognizes the practical approach of measuring the frequency response between voltage reference set point and terminal voltage (Et/Vref) and using the phase characteristic of such frequency response as being the phase characteristic of GEP(s). The phase characteristic of Et/Vref is a better approximation to the phase characteristic of GEP(s) when the frequency response Et/Vref is obtained with the generator synchronized to the grid at its minimum stable power output.

In an effort to allow for reasonable wash-out time constants, the Requirement specifies 0.2 Hz as the applicable threshold. The 0.2 Hz threshold more closely aligns with the observed oscillation frequencies.

A properly tuned PSS should provide positive damping to the local mode of oscillation, which typically has a frequency higher than 1.0 Hz.

This Requirement modifies the requirement associated with the adjustment of the PSS gain. The standard no longer defines the PSS gain in terms of gain margin but instead requires the final PSS gain to be between 1/3 (10 dB) and 1/2 (6 dB) of the maximum practical gain that could be achieved during PSS commissioning. The maximum practical gain might be associated with the excessive noise or raised higher-frequency oscillations in the closed loop response (exciter mode) or any other form if there is inadequate closed-loop performance, as determined during PSS commissioning. It is now part of Measure M3 to show the field test results that led to the determination of the maximum practical gain.

Requirement R4

Requirement R4 requires a Generator Owner to install a PSS on new applicable units or when excitation systems are replaced or retrofitted on existing applicable units. This Requirement applies to new excitation systems and not to existing systems that do not have PSS. The Requirement also allows a reasonable amount of time for the commissioning of new PSS.

Requirement R5

Unlike the language in Requirement R3 that looks *forward* to ensure that a unit is tuned, Requirement R5 looks *backward.* Specifically, the language in Requirement R5, "becoming incapable," indicates the unit was previously capable of meeting the tuning requirements in Requirement R3, but is no longer capable. Restated, Requirement R5 addresses units that were previously working but are now no longer working.

The intent of Requirement R5 is to remove the "tiered" approach to PSS repair/replacement following a failure. A simple, streamlined approach to allow the Generator Owner sufficient time to repair or replace a broken PSS has been written. Consideration has been given for the need to procure parts or new equipment, schedule an equipment/unit outage, and install and test the repaired or replaced PSS. It is recognized that in some instances, it may require (1) replacement of an AVR, and (2) the existence of a PSS, or both the AVR and the PSS may need to be replaced to achieve a functioning system.

The 24-month time frame is sufficient to return a functional, operating PSS to service.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard VAR-501-WECC-3 — Power System Stabilizer

United States

Standard	Requirement	Enforcement Date	Inactive Date
VAR-501-WECC-3	TBD	TBD	