



**ORDER NUMBER
R-19-20**

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. 13
Addressing Reliability Standards for Adoption in British Columbia

BEFORE:

W. M. Everett, QC, Panel Chair
E. B. Lockhart, Commissioner

on September 8, 2020

ORDER

WHEREAS:

- A. On May 1, 2020, the British Columbia Hydro and Power Authority (BC Hydro) filed Mandatory Reliability Standards (MRS) Assessment Report No. 13 (Report 13) with the British Columbia Utilities Commission (BCUC), pursuant to section 125.2(3) of the *Utilities Commission Act* (UCA), assessing one new standard and seven revised standards (collectively, Revised Standards) and considering one retired standard (Retired Standard). The Revised Standards were all developed by the North American Electric Reliability Corporation (NERC) and/or the Western Electricity Coordinating Council (WECC) and approved by the Federal Energy Regulatory Commission (FERC) with an order effective within the period from December 1, 2018 and November 30, 2019 inclusive. The Retired Standard was retired by a FERC order effective within the same time period;
- B. The Revised Standards are all based on defined terms contained in the NERC Glossary of Terms used in Reliability Standards dated August 12, 2019 (NERC Glossary). BC Hydro assessed one new and two revised defined terms (collectively, Revised Terms) contained in the NERC Glossary and considered the retirement of six revised defined terms (collectively, Retired Terms);
- C. In Report 13, BC Hydro recommends that seven of the eight Revised Standards and all three Revised Terms are suitable for adoption in British Columbia (BC) at this time as they will preserve or enhance the reliability of the bulk electric system (BES), and serve the public interest. In addition, BC Hydro recommends that the Retired Standard and all six Retired Terms are suitable for retirement in BC;
- D. The functional registration of the Planning Authority/Planning Coordinator role for the Province of BC remains outstanding. Revised Standard TPL-007-2 contains requirements that pertain to the Planning Coordinator (PC) function and therefore BC Hydro recommends that Reliability Standard TPL-007-2 be held

in abeyance and be of no force or effect in BC until the PC function is resolved, as outlined in detail in Report 13;

- E. BC Hydro recommends that, in connection with the adoption of Revised Standards CIP-003-8, CIP-005-6, CIP-010-3 and CIP-013-1, the BCUC adopt the BC specific versions of the FERC approved Implementation Plans associated with these standards. BC Hydro provided BC specific versions of the CIP-003-8 Implementation Plan and the CIP-005-6/ CIP-010-3/CIP-013-1 joint Implementation Plan as part of Report 13 for the BCUC's consideration;
- F. By Order R-10-20 dated June 4, 2020, BC Hydro was directed to publish a notice of process to the public and entities registered in the MRS Program (Entities) for consideration of the recommendations found in Report 13 along with the established regulatory timetable;
- G. On July 3, 2020, FortisBC Inc. (FBC) submitted that its comments are reflected in BC Hydro's Report 13 and that it has no additional comments;
- H. On July 31, 2020, the BCUC issued information requests (IRs) to BC Hydro and FBC in response to Report 13 and on August 12, 2020, BC Hydro and FBC submitted their respective IR responses;
- I. The BCUC did not review the recoverability of the estimated costs to adopt the Revised Standards or the Revised Terms, and did not review any costs related to the retirement of the Retired Standard or the Retired Terms;
- J. Pursuant to section 125.2(6) of the UCA, the BCUC must adopt the reliability standards addressed in the report if the BCUC considers that the reliability standards are required to maintain or achieve consistency in BC with other jurisdictions that have adopted the reliability standards; and
- K. The BCUC has reviewed and considered Report 13, the Revised Standards, Retired Standard, Revised Terms and Retired Terms assessed therein, comments received from Entities and the responses to IRs and considers that adoption of the recommendations in Report 13 is warranted. Although not assessed by BC Hydro, the BCUC considers that the compliance provisions of the reliability standards (Compliance Provisions) should be adopted to maintain compliance monitoring consistency with other jurisdictions that have adopted the reliability standards with the Compliance Provisions. The BCUC considers it appropriate to provide effective dates for BC Entities to come into compliance with the Revised Standards and Revised Terms adopted in this Order.

NOW THEREFORE pursuant to section 125.2(3) and 125.2(6) of the UCA, which, among other things, 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. Seven of the eight Revised Standards assessed in Report 13 are adopted with effective dates as identified in Table 1 of Attachment A to this Order. Each standard to be superseded by a Revised Standard adopted in this Order shall remain in effect until the effective date of the Revised Standard superseding it.
- 2. Reliability Standard PRC-004-WECC-2 is retired as of the effective date as identified in Table 1 of Attachment A to this Order and Reliability Standard TPL-007-2 is held in abeyance at this time.

3. Attachment B to this Order lists all the reliability standards adopted by the BCUC and effective in BC as of the dates shown. The effective dates for the reliability standards listed in Attachment B supersede the effective dates that were included in any similar list appended to any previous order of the BCUC.
4. 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.
5. The effective date of each of the new or Revised Terms adopted by this order and the date of each retired term is the date in Table 2 of Attachment A to this order.
6. Defined terms set out in the reliability standards bear the same meaning as those set out in the NERC Glossary dated August 12, 2019. Other terms in the NERC Glossary, which do not include a United States FERC approval date on or before November 30, 2018, are of no force or effect in BC.
7. All defined terms listed in Attachment C to this Order are in effect in BC as of the effective dates indicated. 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 made by the BCUC.
8. The Compliance Provisions as defined in the Rules of Procedure for Reliability Standards in British Columbia that accompany each of the adopted reliability standards, are approved in the form directed by the BCUC and as amended from time to time.
9. The BC specific versions of the CIP-003-8 Implementation Plan and the CIP-005-6/CIP-010-3/CIP-013-1 Implementation Plan are adopted in the form directed by the BCUC and as amended from time to time, and effective as indicated in Attachment D to this Order. The BC specific versions of the CIP-003-8 Implementation Plan and CIP-005-6/CIP-010-3/CIP-013-1 Implementation Plan will be posted on the WECC website with links from the BCUC website.
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 adopted in BC are required to report to the BCUC and may, on a voluntary basis, report to NERC or to FERC.

DATED at the City of Vancouver, in the Province of British Columbia, this 8th day of September 2020.

BY ORDER

Original signed by:

W. M. Everett, QC
Commissioner

Attachment

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.	CIP-003-8	Cyber Security – Security Management Controls	October 1, 2020	Revised	CIP-003-7
2.	CIP-005-6	Cyber Security – Electronic Security Perimeter(s)	April 1, 2023	Revised	CIP-005-5
3.	CIP-008-6	Cyber Security – Incident Reporting and Response Planning	April 1, 2023	Revised	CIP-008-5
4.	CIP-010-3	Cyber Security – Configuration Change Management and Vulnerability	April 1, 2023	Revised	CIP-010-2
5.	CIP-013-1	Cyber Security – Supply Chain Risk Management	April 1, 2023	New	N/A; New standard
6.	IRO-002-6	Reliability Coordination – Monitoring and Analysis	April 1, 2021	Revised	IRO-002-5
7.	IRO-006-WECC-3	Qualified Path Unscheduled Flow (USF) Relief	January 1, 2021	Revised	IRO-006-WECC-2
8.	PRC-004-WECC-2	Protection System and Remedial Action Scheme	Retire: September 30, 2021	Retired	N/A; Retired standard
9.	TPL-007-3	Transmission System Planned Performance for Geomagnetic Disturbance Events	N/A – Hold in abeyance	Revised	TPL-007-1 (Held in Abeyance in BC)

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

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.	Contributing Schedule (WECC Regional Term) <i>Glossary term is specific to IRO-006-WECC-2 which will be superseded by IRO-006-WECC-3</i>		Retire: December 31, 2020	Retired (WECC Regional Term)
2.	Cyber Security Incident <i>Glossary term is specific to the revised CIP-003-8 standard</i>		April 1, 2023	Cyber Security Incident
3.	Qualified Controllable Device (WECC Regional Term) <i>Glossary term is specific to IRO-006-WECC-2 which will be superseded by IRO-006-WECC-3</i>		Retire: December 31, 2020	Retired (WECC Regional Term)
4.	Qualified Path (WECC Regional Term) <i>Glossary term is specific to the revised IRO-006-WECC-3 standard</i>		January 1, 2021	N/A; New term
5.	Qualified Transfer Path (WECC Regional Term) <i>Glossary term is specific to IRO-006-WECC-2 which will be superseded by IRO-006-WECC-3</i>		Retire: December 31, 2020	Retired (WECC Regional Term)
6.	Qualified Transfer Path Curtailment Event (WECC Regional Term) <i>Glossary term is specific to IRO-006-WECC-2 which will be superseded by IRO-006-WECC-3</i>		Retire: December 31, 2020	Retired (WECC Regional Term)
7.	Relief Requirement (WECC Regional Term) <i>Glossary term is specific to IRO-006-WECC-2 which will be superseded by IRO-006-WECC-3</i>		Retire: December 31, 2020	Retired (WECC Regional Term)
8.	Reportable Cyber Security Incident <i>Glossary term is specific to the revised CIP-003-8 standard</i>		April 1, 2023	Reportable Cyber Security Incident
9.	Transfer Distribution Factor (WECC Regional Term)	TDF	Retire: December 31, 2020	Retired (WECC Regional Term)

	<i>Glossary term is specific to IRO-006-WECC-2 which will be superseded by IRO-006-WECC-3</i>			
--	---	--	--	--

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 ¹	Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event	R-39-17	January 1, 2018
BAL-002-3	Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event	R-21-19	April 1, 2020
BAL-002-WECC-2a	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-WECC-2 ¹	Automatic Time Error Correction	R-32-14	October 1, 2014
BAL-004-WECC-3	Automatic Time Error Correction	R-21-19	January 1, 2020
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
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	R-33-18	October 1, 2018 and as per BC-specific Implementation Plan
CIP-003-7 ¹	Cyber Security — Security Management Controls	R-21-19	October 1, 2019 and as per BC-specific Implementation Plan
CIP-003-8	Cyber Security — Security Management Controls	R-19-20	October 1, 2020 and as per BC-specific Implementation Plan
CIP-004-6	Cyber Security — Personnel & Training	R-39-17	October 1, 2018 and as per BC-specific Implementation Plan
CIP-005-5 ¹	Cyber Security – Electronic Security Perimeter(s)	R-38-15	October 1, 2018 and as per BC-specific Implementation Plan
CIP-005-6	Cyber Security – Electronic Security Perimeter(s)	R-19-20	April 1, 2023 and as per BC-specific Implementation Plan

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

² On November 21, 2013, FERC Order 788 (referred to as Paragraph 81) approved the retiring of the reliability standard requirements.

Standard	Name	BCUC Order Adopting	Effective Date
CIP-006-6	Cyber Security — Physical Security of BES Cyber Systems	R-39-17	October 1, 2018 and as per BC-specific Implementation Plan
CIP-007-6	Cyber Security — System Security Management	R-39-17	October 1, 2018 and as per BC-specific Implementation Plan
CIP-008-5 ¹	Cyber Security – Incident Reporting and Response Planning	R-38-15	October 1, 2018 and as per BC-specific Implementation Plan
CIP-008-6	Cyber Security – Incident Reporting and Response Planning	R-19-20	April 1, 2023
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	R-39-17	October 1, 2018 and as per BC-specific Implementation Plan
CIP-010-2 ¹	Cyber Security – Configuration Change Management and Vulnerability Assessments	R-39-17	October 1, 2018 and as per BC-specific Implementation Plan
CIP-010-3	Cyber Security – Configuration Change Management and Vulnerability Assessments	R-19-20	April 1, 2023 and as per BC-specific Implementation Plan
CIP-011-2	Cyber Security – Information Protection	R-39-17	October 1, 2018 and as per BC-specific Implementation Plan
CIP-013-1	Cyber Security - Supply Chain Risk Management	R-19-20	April 1, 2023 and as per BC-specific Implementation Plan
CIP-014-2	Physical Security	R-32-16A	October 1, 2017 and as per BC-specific Implementation Plan
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-003-1 ³	Load Shedding Plans	G-67-09	November 1, 2010
EOP-003-2 ⁴	Load Shedding Plans	n/a	Adoption held in abeyance at this time ⁵
EOP-004-3 ¹	Event Reporting	R-39-17	October 1, 2017
EOP-004-4	Event Reporting	R-21-19	October 1, 2020

³ Reliability standard would be superseded by EOP-003-2 if adopted in BC Adoption of EOP-003-2 pending reassessment.

⁴ Reliability standard is superseded by EOP-011-1 as of the EOP-011-1 effective date in conjunction with PRC-010-2 Requirement 1 if adopted in BC Adoption of PRC-010-2 pending reassessment.

⁵ Unable to assess based on undefined Planning Coordinator/Planning Authority footprints and entities responsible. The BCUC Reasons for Decision for Order R-41-13 (page 20), indicated that a separate process would be established to consider this matter as it pertains to BC.

Standard	Name	BCUC Order Adopting	Effective Date
EOP-005-2 ¹	System Restoration and Blackstart Resources	R-32-14	August 1, 2015 R3.1: Retired January 21, 2014 ²
EOP-005-3	System Restoration and Blackstart Resources	R-21-19	October 1, 2020
EOP-006-2 ¹	System Restoration Coordination	R-32-14	August 1, 2014
EOP-006-3	System Restoration Coordination	R-21-19	October 1, 2020
EOP-008-1 ¹	Loss of Control Center Functionality	R-32-14	August 1, 2015
EOP-008-2	Loss of Control Center Functionality	R-21-19	October 1, 2020
EOP-010-1 ⁶	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-008-3	Facility Ratings	R-32-14	August 1, 2015 R4 and 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 ⁷	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 ⁵
FAC-014-2	Establish and Communicate System Operating Limits	G-167-10	January 1, 2011
FAC-501-WECC-1 ¹	Transmission Maintenance	R-1-13	April 15, 2013

⁶ Requirement 2 of the reliability standard will be effective upon the retirement of IRO-005-3.1a Requirement 3 which follows the effective date of IRO-002-4 (October 1, 2017; per BCUC Order R-39-17).

⁷ 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
FAC-501-WECC-2	Transmission Maintenance	R-21-19	October 1, 2019
INT-004-3.1	Dynamic Transfers	R-38-15	R1, R2: October 1, 2015 R3: January 1, 2016
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 ⁸	Reliability Coordination – Facilities	R-1-13	April 15, 2013
IRO-002-5 ¹	Reliability Coordination – Monitoring and Analysis	R-33-18	January 1, 2019
IRO-002-6	Reliability Coordination – Monitoring and Analysis	R-19-20	April 1, 2021
IRO-005-3.1a ^{8,9}	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 ¹	Qualified Transfer Path Unscheduled Flow (USF) Relief	R-38-15	October 1, 2015
IRO-006-WECC-3	Qualified Transfer Path Unscheduled Flow (USF) Relief	R-19-20	January 1, 2021
IRO-008-2	Reliability Coordinator Operational Analyses and Real-time Assessments	R-39-17	October 1, 2017
IRO-009-2	Reliability Coordinator Actions to Operate Within IROs	R-39-17	October 1, 2017
IRO-010-2	Reliability Coordinator Data Specification and Collection	R-39-17	April 1, 2019
IRO-014-3	Coordination Among Reliability Coordinators	R-39-17	October 1, 2017
IRO-015-1 ⁸	Notification and Information Exchange	G-67-09	November 1, 2010
IRO-017-1	Outage Coordination	R-39-17	October 1, 2020

⁸ Refer to “IRO and TOP Reliability Standards Supersession Mapping” section below.

⁹ Requirement 3 of the reliability standard is superseded by EOP-010-1 Requirement 2 as of the IRO-002-4 effective date (October 1, 2017; per BCUC Order R-39-17).

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 ¹⁰	Steady-State Data for Modeling and Simulation for the Interconnected Transmission System	G-67-09	November 1, 2010
MOD-012-0 ¹⁰	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 With revised effective dates by Order R-14-20	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by April 1, 2021
MOD-026-1	Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions	R-38-15	R1: October 1, 2016 R2: 30% by October 1, 2019 50% by October 1, 2021 100% by October 1, 2025 R3-R6: October 1, 2015
MOD-027-1	Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions	R-38-15	R1: October 1, 2016 R2: 30% by October 1, 2019 50% by October 1, 2021 100% by October 1, 2025 R3-R5: October 1, 2015
MOD-028-2	Area Interchange Methodology	R-32-14	August 1, 2014
MOD-029-2a	Rated System Path Methodology	R-39-17	October 1, 2017
MOD-030-3	Flowgate Methodology	R-39-17	October 1, 2017

¹⁰ 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
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 ⁵
MOD-033-1	Steady-State and Dynamic System Model Validation	R-38-15	Effective date held in abeyance ⁵
NUC-001-3	Nuclear Plant Interface Coordination	R-38-15	January 1, 2016
PER-001-0.2 ⁸	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 ¹	Operating Personnel Credentials	R-41-13	January 1, 2015
PER-003-2	Operating Personnel Credentials	R-21-19	April 1, 2020
PER-004-2 ¹¹	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
PER-006-1 ¹²	Specific Training for Personnel	R-21-19	October 1, 2021
PRC-001-1.1(ii) ¹³	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 Retirement: September 30, 2021
PRC-005-1.1b ^{1, 16}	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

¹¹ Reliability standard will be superseded by PER-003-2 if adopted in BC as of the PER-003-2 effective date.

¹² Reliability standard will supersede PRC-001-1.1(ii) R1 as of the effective date of PER-006-1.

¹³ PRC-001-1.1(ii) Requirement 1 will be superseded by PER-006-1 as of the effective date of PER-006-1; PRC-001-1(ii) Requirements 3 and 4 will be superseded by PRC-027-1 as of the effective date of PRC-027-1; and, the rest of PRC-001-1.1(ii) will be superseded by other reliability standards as of October 1, 2020.

Standard	Name	BCUC Order Adopting	Effective Date
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-006-3 ¹⁴	Automatic Underfrequency Load Shedding	n/a	Adoption held in abeyance at this time ⁵
PRC-007-0 ¹⁵	Assuring consistency of entity Underfrequency Load Shedding Program Requirements	G-67-09	November 1, 2010
PRC-008-0 ¹⁶	Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program	G-67-09	November 1, 2010
PRC-009-0 ¹⁵	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	n/a	Adoption held in abeyance at this time ⁵
PRC-011-0 ¹⁶	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. ⁵ R2: Attachment 2, Section I Parts 7(d) and 7(e) to be determined. Unable to be assessed at this time. ⁵ R4: To be determined. Unable to be assessed at this time. ⁵
PRC-015-1 ¹⁷	Remedial Action Scheme Data and Documentation	R-39-17	October 1, 2017

¹⁴ Reliability standard supersedes PRC-006-1 and PRC-006-2 which have both been held in abeyance due to the undefined Planning Coordinator/Planning Authority footprints and entities responsible.

¹⁵ Reliability standard will be superseded by PRC-006-3 if adopted in BC Adoption of PRC-006-3 pending reassessment.

¹⁶ Reliability standard is superseded by PRC-005-6 as per the PRC-005-6 BC-specific Implementation Plan.

¹⁷ Reliability standard is superseded by PRC-012-2 as of the PRC-012-2 effective date.

Standard	Name	BCUC Order Adopting	Effective Date
PRC-016-1 ¹⁷	Remedial Action Scheme Misoperations	R-39-17	October 1, 2017
PRC-017-1 ¹⁶	Remedial Action Scheme Maintenance and Testing	R-39-17	October 1, 2017
PRC-018-1 ¹⁸	Disturbance Monitoring Equipment Installation and Data Reporting	G-67-09	November 1, 2010
PRC-019-2	Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection	R-32-16A With revised effective dates by Order R-14-20	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by April 1, 2021
PRC-021-1 ¹⁹	Under Voltage Load Shedding Program Data	G-67-09	November 1, 2010
PRC-022-1 ¹⁹	Under Voltage Load Shedding Program Performance	G-67-09	November 1, 2010 R2: Retired January 21, 2014 ²
PRC-023-2 ^{1, 20}	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 ⁵ R6: To be determined ⁵
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 With revised effective dates by Order R-14-20	40% by October 1, 2017 60% by October 1, 2018 80% by October 1, 2019 100% by April 1, 2021

¹⁸ Reliability standard is superseded by PRC-002-2 as of the PRC-002-2 effective date.

¹⁹ Reliability standard is superseded by PRC-010-2 if adopted in BC Adoption of PRC-010-2 pending reassessment.

²⁰ PRC-023-2 Requirement 1, Criterion 6 only is superseded by PRC-025-1 as of PRC-025-1's 100 per cent Effective Date.

Standard	Name	BCUC Order Adopting	Effective Date
PRC-025-1 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-025-2	Generator Relay Loadability	R-21-19	October 1, 2019
PRC-026-1	Relay Performance During Stable Power Swings	n/a	Adoption held in abeyance at this time ⁵
PRC-027-1 ²¹	Coordination of Protection Systems for Performance During Faults	R-21-19	October 1, 2021
TOP-001-1a ⁸	Reliability Responsibilities and Authorities	R-1-13	January 15, 2013
TOP-001-4	Transmission Operations	R-33-18 With revised effective dates by Order R-14-20	April 1, 2021
TOP-002-2.1b ⁸	Normal Operations Planning	R-41-13	December 12, 2013
TOP-002-4	Operations Planning	R-39-17 With revised effective dates by Order R-14-20	April 1, 2021
TOP-003-1 ⁸	Planned Outage Coordination	R-1-13	April 15, 2013
TOP-003-3	Operational Reliability Data	R-39-17	April 1, 2019
TOP-004-2 ⁸	Transmission Operations	G-167-10	January 1, 2011
TOP-005-2a ⁸	Operational Reliability Information	R-1-13	April 15, 2013
TOP-006-2 ⁸	Monitoring System Conditions	R-1-13	April 15, 2013
TOP-007-0 ⁸	Reporting System Operating Unit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations	G-67-09	November 1, 2010
TOP-008-1 ⁸	Response to Transmission Limit Violations	G-67-09	November 1, 2010
TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities	R-33-18 With revised effective dates by Order R-14-20	April 1, 2021
TPL-001-0.1 ²²	System Performance Under Normal (No Contingency) Conditions (Category A)	G-167-10	January 1, 2011

²¹ Reliability standard will supersede PRC-001-1.1(ii) Requirements 3 and 4 as of the effective date of PRC-027-1.

²² Reliability standard is superseded by TPL-001-4 Requirements 2 to 6, and 8 as of their effective dates.

Standard	Name	BCUC Order Adopting	Effective Date
TPL-001-4	Transmission System Planning Performance Requirements	R-27-18A	R1: July 1, 2019 R2-R6, R8: July 1, 2020 R7: To be determined ⁵
TPL-002-0b ²²	System Performance Following Loss of a Single Bulk Electric System Element (Category B)	R-1-13	January 15, 2013
TPL-003-0b ²²	System Performance Following Loss of Two or More Bulk Electric System Elements (Category C)	R-32-14	August 1, 2014
TPL-004-0a ²²	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 ¹	Transmission System Planned Performance for Geomagnetic Disturbance Events	N/A	Adoption held in abeyance at this time ⁵
TPL-007-3	Transmission System Planned Performance for Geomagnetic Disturbance Events	N/A	Adoption held in abeyance at this time ⁵
VAR-001-4.2 ¹	Voltage and Reactive Control	R-33-18	October 1, 2018
VAR-001-5	Voltage and Reactive Control	R-21-19	October 1, 2019
VAR-002-4.1	Generator Operation for Maintaining Network Voltage Schedules	R-33-18	October 1, 2018
VAR-501-WECC-2 ¹	Power System Stabilizer (PSS)	R-32-16A	October 1, 2016
VAR-501-WECC-3.1	Power System Stabilizer (PSS)	R-33-18	October 1, 2020 R3: For units placed into service after the effective date: January 1, 2021 For units placed into service prior 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-002-2	—	Reliability Coordination - Facilities
IRO-005-3.1a	—	Reliability Coordination - Current Day Operations
IRO-015-1	—	Notifications and Information Exchange 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-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-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

Standard IRO-005-3.1a — Reliability Coordination - Current Day Operations	
Requirement Being Superseded	Superseding BCUC Approved Standard(s)
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-001-4
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-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 PER-001-0.2 — Operating Personnel Responsibility and Authority	
Requirement Being Superseded	Superseding BCUC Approved Standard(s)
All Requirements	TOP-001-4

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

Standard TOP-002-2.1b — Normal Operations Planning	
Requirement Being Superseded	Superseding BCUC Approved Standard(s)
Requirement R1	TOP-001-4 TOP-002-4
Requirements R2, R5-R9, 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-001-4 TOP-002-4 TOP-003-3
Requirement R11	TOP-001-4 TOP-002-4
Requirement R13	TOP-001-4 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-001-4
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-001-4
Requirement R2	TOP-001-4 TOP-002-4
Requirements R3 and R4	TOP-001-4
Requirement R5	Retired
Requirement R6	IRO-017-1 TOP-001-4

Standard TOP-005-2a — Operational Reliability Information	
Requirement Being Superseded	Superseding BCUC Approved Standard(s)
Requirement R1	<p>IRO-010-2</p> <p>TOP-003-3</p>
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	<p>IRO-010-2</p> <p>TOP-001-4</p> <p>TOP-003-3</p>
Requirement R2	<p>IRO-002-4</p> <p>TOP-001-4</p>
Requirement R3	<p>IRO-010-2</p> <p>TOP-003-3</p>
Requirement R4	TOP-003-3
Requirement R5	<p>IRO-002-5</p> <p>TOP-001-4</p>
Requirement R6	TOP-003-3

Standard TOP-006-2 — Monitoring System Conditions	
Requirement Being Superseded	Superseding BCUC Approved Standard(s)
Requirement R7	<p>IRO-002-5</p> <p>TOP-001-4</p>

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	<p>IRO-008-2</p> <p>TOP-001-4</p>
Requirement R2	<p>IRO-009-2</p> <p>TOP-001-4</p>
Requirement R3	<p>EOP-003-2, Requirement 1 (adoption held in abeyance in BC due to PA/PC dependencies)</p> <p>IRO-009-2</p>
Requirement R4	<p>IRO-008-2</p>

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-001-4
Requirements R2 and R3	TOP-001-4
Requirement R4	TOP-001-4 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-19-20, dated September 8, 2020

Introduction:

This document is to be used in conjunction with the NERC Glossary dated August 12, 2019.

- 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, 2019 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 August 12, 2019 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 (N _{IA})	-	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 (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.

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.

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

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Composite Protection System	-	Report No. 9	R-32-16A	Adoption	October 1, 2017
Consequential Load Loss	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Contingency Event Recovery Period ¹	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Contingency Reserve ¹	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Contingency Reserve Restoration Period ¹	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Contributing Schedule (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020
Control Center	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Critical Assets	-	Report No. 9	R-32-16A	Retirement	September 30, 2018
Critical Cyber Assets	-	Report No. 9	R-32-16A	Retirement	September 30, 2018
Cyber Assets	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Cyber Security Incident	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Cyber Security Incident	-	Report No. 13	R-19-20	Adoption	April 1, 2023
Demand-Side Management	DSM	Report No. 9	R-32-16A	Adoption	October 1, 2016

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Dial-up Connectivity	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Distribution Provider	DP	Report No. 10	R-39-17	Adoption	October 1, 2017
Disturbance	-	Report No. 11	R-33-18	Retirement	October 1, 2018
Dynamic Interchange Schedule or Dynamic Schedule	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Electronic Access Control or Monitoring Systems	EACMS	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Electronic Access Point	EAP	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Electronic Security Perimeter	ESP	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Element	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Energy Emergency ²	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Energy Emergency	-	Report No. 11	R-33-18	Retirement	October 1, 2018
External Routable Connectivity	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Frequency Bias Setting	-	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Frequency Response Measure	FRM	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced
Frequency Response Obligation	FRO	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced
Frequency Response Sharing Group	FRSG	Report No. 8	R-38-15	Adoption	Align with earliest effective date of BAL-003-1 standard where this term is referenced
Generator Operator	GOP	Report No. 10	R-39-17	Adoption	October 1, 2017
Generator Owner	GO	Report No. 10	R-39-17	Adoption	October 1, 2017
Geomagnetic Disturbance Vulnerability Assessment or GMD Vulnerability Assessment	GMD	Report No. 10	R-39-17	Adoption	To be determined ³
Interactive Remote Access	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Interchange Authority	IA	Report No. 10	R-39-17	Adoption	October 1, 2017
Interchange Meter Error (IME)	-	Report No. 11	R-33-18	Adoption	October 1, 2019
Interconnected Operations Service	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Interconnection	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Interconnection Reliability Operating Limit	IROL	Report No. 6	R-41-13	Adoption	December 12, 2013
Intermediate Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Intermediate System	-	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.

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

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Interpersonal Communication	-	Report No. 9	R-32-16A	Adoption	October 1, 2017
Load-Serving Entity	LSE	Report No. 10	R-39-17	Adoption	October 1, 2017
Long-Term Transmission Planning Horizon	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Minimum Vegetation Clearance Distance	MVCD	Report No. 7	R-32-14	Adoption	August 1, 2015
Misoperation	-	Report No. 9	R-32-16A	Adoption	October 1, 2017
Most Severe Single Contingency ¹	MSSC	Report No. 10	R-39-17	Adoption	January 1, 2018
Native Balancing Authority	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Non-Consequential Load Loss	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Non-Spinning Reserve	-	Report No. 11	R-33-18	Retirement	October 1, 2018
Operating Instruction	-	Report No. 9	R-32-16A	Adoption	April 1, 2017
Operational Planning Analysis ²	-	Report No. 6	R-41-13	Adoption	December 12, 2013
Operational Planning Analysis ²	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Operational Planning Analysis ²	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Operational Planning Analysis	OPA	Report No. 12	R-21-19	Adoption	October 1, 2021
Operations Support Personnel	-	Report No. 8	R-38-15	Adoption	Align with effective date of Requirement 5 of the PER-005-2 standard where this term is referenced
Physical Access Control Systems	PACS	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Physical Security Perimeter	PSP	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Planning Assessment	-	TPL-001-4	R-27-18A	Adoption	July 1, 2019
Planning Authority	PA	Report No. 10	R-39-17	Adoption	October 1, 2017
Point of Receipt	POR	Report No. 10	R-39-17	Adoption	October 1, 2017
Pre-Reporting Contingency Event ACE Value ¹	-	Report No. 10	R-39-17	Adoption	January 1, 2018
Protected Cyber Assets ²	PCA	Report No. 8	R-38-15	Adoption	Align with effective date of CIP Version 5 standards (CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1) where this term is referenced.
Protected Cyber Assets	PCA	Report No. 10	R-39-17	Adoption	October 1, 2018
Protection System	-	Report No. 6	R-41-13	Adoption	January 1, 2015 for each entity to modify its protection system maintenance and testing program to reflect the new definition (to coincide with recommended effective date of PRC-005-1b) and until the end of the first complete maintenance and testing cycle to implement any additional maintenance and testing for battery chargers as required by that entity's program.
Protection System Coordination Study	-	Report No. 12	R-21-19	Adoption	October 1, 2021
Protection System Maintenance Program	PSMP	Report No. 8	R-38-15	Adoption	Align with effective date of Requirement 1 of the PRC-005-2 standard where this term is referenced
Protection System Maintenance Program (<i>PRC-005-6</i>)	PSMP	Report No. 10	R-39-17	Adoption	October 1, 2019
Pseudo-Tie ²	-	Report No. 8	R-38-15	Adoption	October 1, 2015
Pseudo-Tie	-	Report No. 11	R-33-18	Adoption	January 1, 2019
Qualified Controllable Device (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020
Qualified Path (WECC Regional Term)	-	Report No. 13	R-19-20	Adoption	January 1, 2021
Qualified Transfer Path (WECC Regional Term)	-	Report No. 13	R-19-20	Retirement	December 31, 2020

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

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

NERC Glossary Term	Acronym	Assessment Report Number	BCUC Order Number	BCUC Adoption or Retirement	Effective Date
Total Internal Demand	-	Report No. 9	R-32-16A	Adoption	October 1, 2016
Transient Cyber Asset ²	-	Report No. 10	R-39-17	Adoption	October 1, 2018
Transient Cyber Asset	TCA	Report No. 12	R-21-19	Adoption	October 1, 2019
Transmission Customer	-	Report No. 10	R-39-17	Adoption	October 1, 2017
Transfer Distribution Factor (WECC Regional Term)	TDF	Report No. 13	R-19-20	Retirement	December 31, 2020
Transmission Operator	TOP	Report No. 10	R-39-17	Adoption	October 1, 2017
Transmission Owner	TO	Report No. 10	R-39-17	Adoption	October 1, 2017
Transmission Planner	TP	Report No. 10	R-39-17	Adoption	October 1, 2017
Transmission Service Provider	TSP	Report No. 10	R-39-17	Adoption	October 1, 2017
Under Voltage Load Shedding Program	-	Report No. 9		-	To be determined ³
Right-of-Way	ROW	Report No. 7	R-32-14	Adoption	August 1, 2015
TLR (Transmission Loading Relief) Log	-	Report No. 7	R-32-14	Adoption	August 1, 2014
Vegetation Inspection	-	Report No. 7	R-32-14	Adoption	August 1, 2015

Table 2 NERC Glossary Adoption History in BC

NERC Glossary of Terms Version Date	Assessment Report Number	BCUC Order Adoption Date	BCUC Order Adopting	Notes Pertaining to NERC Glossary Effective Date
February 12, 2008	Report No. 1	June 4, 2009	G-67-09	<ol style="list-style-type: none"> 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	TPL-001-4	June 28, 2018	R-27-18A	

NERC Glossary of Terms Version Date	Assessment Report Number	BCUC Order Adoption Date	BCUC Order Adopting	Notes Pertaining to NERC Glossary Effective Date
October 6, 2017	Report No. 11	October 1, 2018	R-33-18	
July 3, 2018	Report No.12	September 26, 2019	R-21-19	
August 12, 2019	Report No. 13	September 8, 2020	R-19-20	

**British Columbia Utilities Commission (BCUC)
Implementation Plan for Reliability Standard CIP-003-8
Cyber Security – Security Management Controls**

Applicable Standard

- Reliability Standard CIP-003-8 - Cyber Security – Security Management Controls

Requested Retirements

- Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls

Applicable Entities

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

Effective Dates

Reliability Standard CIP-003-8

The Reliability Standard CIP-003-8 shall become effective immediately after the BCUC's order approving the standard with the following exceptions for initial compliance (as replicated from the BCUC Implementation Plan for CIP-003-7 under Order No. R-21-19):

Compliance Date for CIP-003-8, Requirement R1, Parts 1.2.2 and 1.2.3 and Requirement R2 (in reference to Attachment 1, Sections 2 and 3):

- Registered Entities shall not be required to comply until October 1, 2023

Compliance Date for CIP-003-8, Requirement R1, Parts 1.2.5 and 1.2.6 and Requirement R2 (in reference to Attachment 1, Sections 1, 4 and 5):

- Registered Entities shall not be required to comply until October 1, 2021.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5 (or any subsequent version of that Reliability Standard) which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP- 002-5, Attachment 1, criteria.

For planned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 on the update of the identification and categorization of the affected BES Cyber System.

For unplanned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 according to the following timelines, following the identification and categorization of the affected BES Cyber System.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 Months
New medium impact BES Cyber System	12 Months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium- Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 Months
Responsible entity identifies first medium impact or High impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP 002-5 identification and categorization processes)	24 Months

Unplanned Changes Resulting in Low Impact Categorization

For unplanned changes resulting in a Low Impact BES Cyber System categorization where previously the asset containing Cyber Assets had no categorization, the Responsible Entity shall comply with all Requirements applicable to Low Impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-7

Reliability Standard CIP-003-7 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-8 in British Columbia.

British Columbia Utilities Commission(BCUC)
Implementation Plan Cyber Security Supply Chain Risk Management
Associated Reliability Standards

Applicable Standard(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-5 — Cyber Security — Electronic Security Perimeters
- CIP-010-2 — Configuration Change Management and Vulnerability Assessments

Prerequisite Standard(s)

None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator

- Transmission Operator
- Transmission Owner

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 apply only to BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

General Considerations

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-1.

Effective Date

For each of the CIP-005-6, CIP-010-3, and CIP-013-1 Reliability Standards

The Reliability Standard shall become effective on the first day of the first calendar quarter that is 30 months after the effective date of the BCUC's order approving the Reliability Standard.

Initial Performance of Periodic Requirements

CIP-013-1 Requirement R3

The initial review and approval of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement R3 must be completed on or before the effective date of CIP-013-1.

Planned or Unplanned Changes Resulting in a Higher Categorization

Compliance timelines with CIP-005-6, CIP-010-3, and CIP-013-1 for planned or unplanned changes in categorization are consistent with the BCUC Implementation Plan associated with the CIP Version 5 standards per BCUC Order R-38-15.

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5 (or any subsequent version of that Reliability Standard) which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber

System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For planned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 on the update of the identification and categorization of the affected BES Cyber System.

For unplanned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 according to the following timelines, following the identification and categorization of the affected BES Cyber System.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 Months
New medium impact BES Cyber System	12 Months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 Months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 Months

Retirement Date

Standards listed in the **Requested Retirement(s)** section shall be retired immediately prior to the effective date of the CIP-005-6, CIP-010-3, and CIP-013-1 standards in British Columbia.

CIP-003-8 - Cyber Security — Security Management Controls

A. Introduction

- 1. Title:** Cyber Security — Security Management Controls
- 2. Number:** CIP-003-8
- 3. Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- 4. Applicability:**
 - 4.1. Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. Balancing Authority**
 - 4.1.2. Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1.** Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2.** Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3.** Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4.** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. Generator Operator**
 - 4.1.4. Generator Owner**
 - 4.1.5. Reliability Coordinator**
 - 4.1.6. Transmission Operator**

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

- 4.2.1.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.2.1.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-8:

- 4.2.3.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
- 4.2.3.2.** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
- 4.2.3.3.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.4.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates*:

See Implementation Plan for CIP-003-8.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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

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

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

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

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

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

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS

CIP-003-8 - Cyber Security — Security Management Controls

tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

- R1.** Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- 1.1.** For its high impact and medium impact BES Cyber Systems, if any:
 - 1.1.1.** Personnel and training (CIP-004);
 - 1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
 - 1.1.3.** Physical security of BES Cyber Systems (CIP-006);
 - 1.1.4.** System security management (CIP-007);
 - 1.1.5.** Incident reporting and response planning (CIP-008);
 - 1.1.6.** Recovery plans for BES Cyber Systems (CIP-009);
 - 1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
 - 1.1.8.** Information protection (CIP-011); and
 - 1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
 - 1.2.** For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
 - 1.2.1.** Cyber security awareness;
 - 1.2.2.** Physical security controls;
 - 1.2.3.** Electronic access controls;
 - 1.2.4.** Cyber Security Incident response;
 - 1.2.5.** Transient Cyber Assets and Removable Media malicious code risk mitigation; and
 - 1.2.6.** Declaring and responding to CIP Exceptional Circumstances.
- M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.
- R2.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

CIP-003-8 - Cyber Security — Security Management Controls

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

- M2.** Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.
- R3.** Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium]*
[Time Horizon: Operations Planning]
- M3.** An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.
- R4.** The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower]* *[Time Horizon: Operations Planning]*
- M4.** An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.4. Additional Compliance Information:

None.

CIP-003-8 - Cyber Security — Security Management Controls

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1)</p> <p>OR</p> <p>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</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1)</p> <p>OR</p> <p>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</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1)</p> <p>OR</p> <p>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</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1)</p> <p>OR</p> <p>The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1)</p> <p>OR</p> <p>The Responsible Entity did not</p>

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>complete this review in less than or equal to 16 calendar months of the previous review. (R1.1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1)</p>	<p>complete this review in less than or equal to 17 calendar months of the previous review. (R1.1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1)</p>	<p>calendar months of the previous review. (R1.1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)</p> <p>OR</p> <p>The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact</p>	<p>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)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1)</p> <p>OR</p>

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>OR</p> <p>The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar</p>	<p>OR</p> <p>The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar</p>	<p>BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its</p>	<p>The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the six topics required by R1. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not</p>

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of</p>	<p>months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17</p>	<p>assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)</p>	<p>complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)</p>

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.2)	calendar months of the previous approval. (R1.2)		
R2	Operations Planning	Lower	<p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2)</p> <p>OR</p> <p>The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2,</p>	<p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed</p>	<p>The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic</p>	<p>The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)</p>

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>Attachment 1, Section 3. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing</p>	<p>to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for electronic access controls but</p>	<p>access controls according to Requirement R2, Attachment 1, Section 3.1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented the determination of</p>	

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented</p>	<p>failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents</p>	<p>whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,</p>	

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	<p>according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2,</p>	<p>Attachment 1, Section 5.1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for</p>	

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber</p>	<p>the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)</p>	

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2,		

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.3. (R2)		
R3	Operations Planning	Medium	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this 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 change. (R3)	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 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	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	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	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process

CIP-003-8 - Cyber Security — Security Management Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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)	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)	within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	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 change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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.

CIP-003-8 - Cyber Security — Security Management Controls

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

CIP-003-8 - Cyber Security — Security Management Controls

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

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

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

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

- 4.1** Identification, classification, and response to Cyber Security Incidents;
- 4.2** Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the

CIP-003-8 - Cyber Security — Security Management Controls

Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

- 43** Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- 44** Incident handling for Cyber Security Incidents;
- 45** Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and
- 46** Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

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

- 5.1** For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):
 - Antivirus software, including manual or managed updates of signatures or patterns;
 - Application whitelisting; or
 - Other method(s) to mitigate the introduction of malicious code.
- 5.2** For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:
 - 5.2.1** Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):
 - Review of antivirus update level;
 - Review of antivirus update process used by the party;
 - Review of application whitelisting used by the party;
 - Review use of live operating system and software executable only from read-only media;
 - Review of system hardening used by the party; or

- Other method(s) to mitigate the introduction of malicious code.

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

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

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
 - a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
 - b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

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

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

CIP-003-8 - Cyber Security — Security Management Controls

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

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

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

CIP-003-8 Supplemental Material

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

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

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

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

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

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

1.1.4 System security management (CIP-007)

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

CIP-003-8 Supplemental Material

- 1.1.5 Incident reporting and response planning (CIP-008)
 - Recognition of Cyber Security Incidents
 - Appropriate notifications upon discovery of an incident
 - Obligations to report Cyber Security Incidents
- 1.1.6 Recovery plans for BES Cyber Systems (CIP-009)
 - Availability of spare components
 - Availability of system backups
- 1.1.7 Configuration change management and vulnerability assessments (CIP-010)
 - Initiation of change requests
 - Approval of changes
 - Break-fix processes
- 1.1.8 Information protection (CIP-011)
 - Information access control methods
 - Notification of unauthorized information disclosure
 - Information access on a need-to-know basis
- 1.1.9 Declaring and responding to CIP Exceptional Circumstances
 - Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
 - Processes to allow for exceptions to policy that do not violate CIP requirements

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

- 1.2.1 Cyber security awareness
 - Method(s) for delivery of security awareness
 - Identification of groups to receive cyber security awareness
- 1.2.2 Physical security controls
 - Acceptable approach(es) for selection of physical security control(s)
- 1.2.3 Electronic access controls
 - Acceptable approach(es) for selection of electronic access control(s)
- 1.2.4 Cyber Security Incident response
 - Recognition of Cyber Security Incidents

CIP-003-8 Supplemental Material

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

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

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

Requirement R2:

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

CIP-003-8 Supplemental Material

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate “how” the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

CIP-003-8 Supplemental Material

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

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

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

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

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

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

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

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

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

CIP-003-8 Supplemental Material

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

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

Electronic Access Control Exclusion

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

Considerations for Determining Routable Protocol Communications

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

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

CIP-003-8 Supplemental Material

at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

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

Concept Diagrams

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

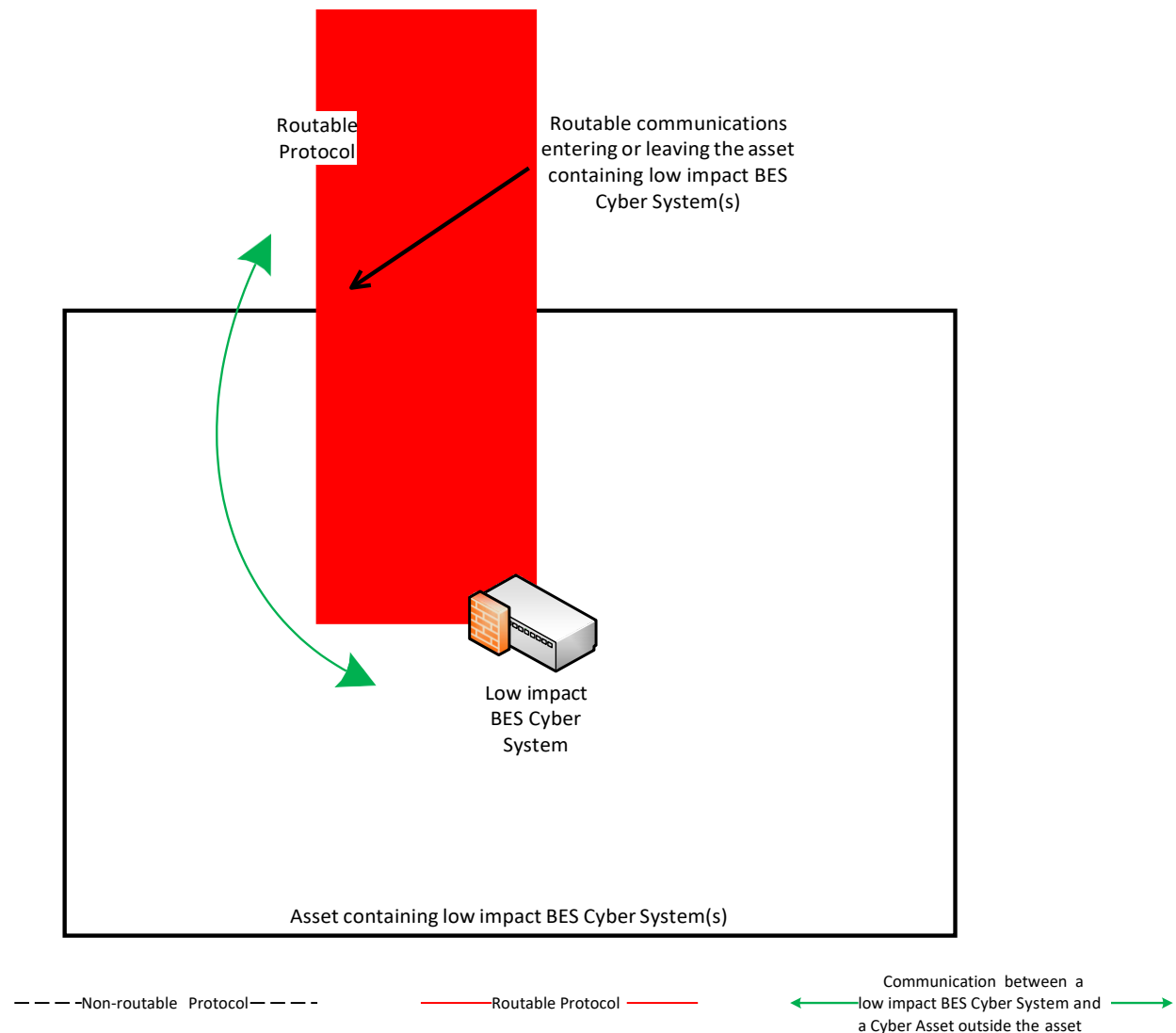
NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

CIP-003-8 Supplemental Material

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

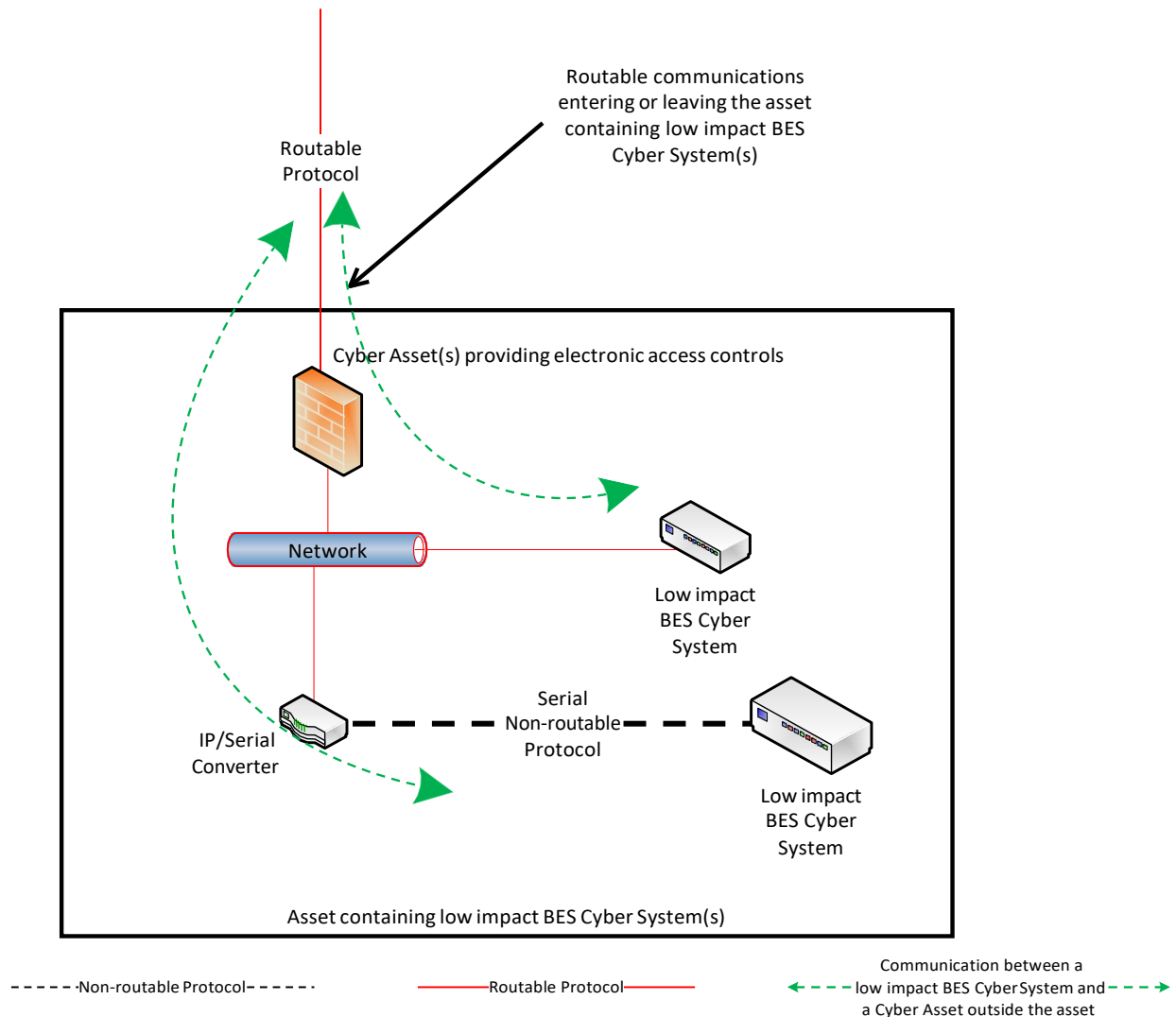
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s)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

*Reference Model 1*

CIP-003-8 Supplemental Material

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

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

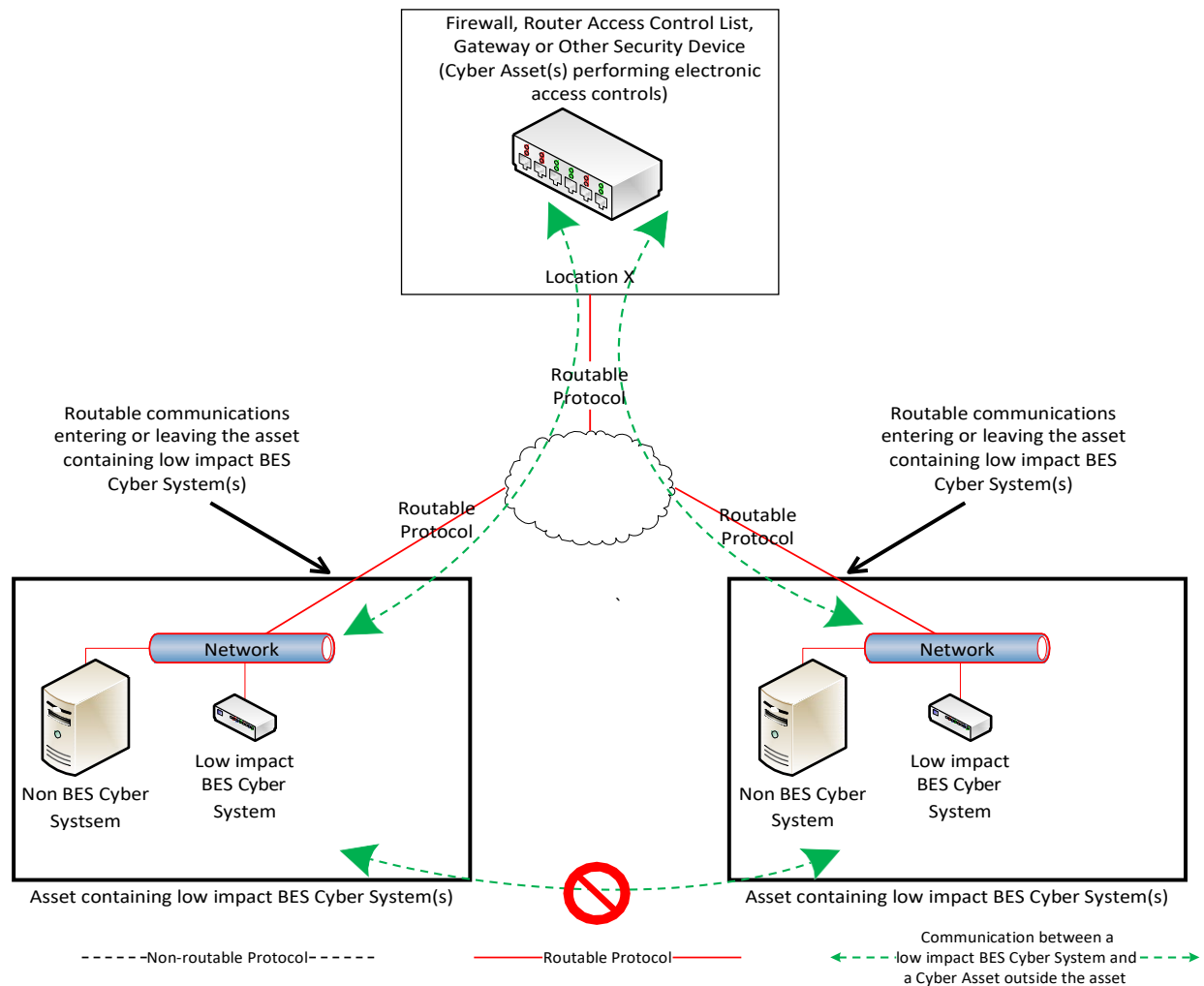


Reference Model 2

CIP-003-8 Supplemental Material

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

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

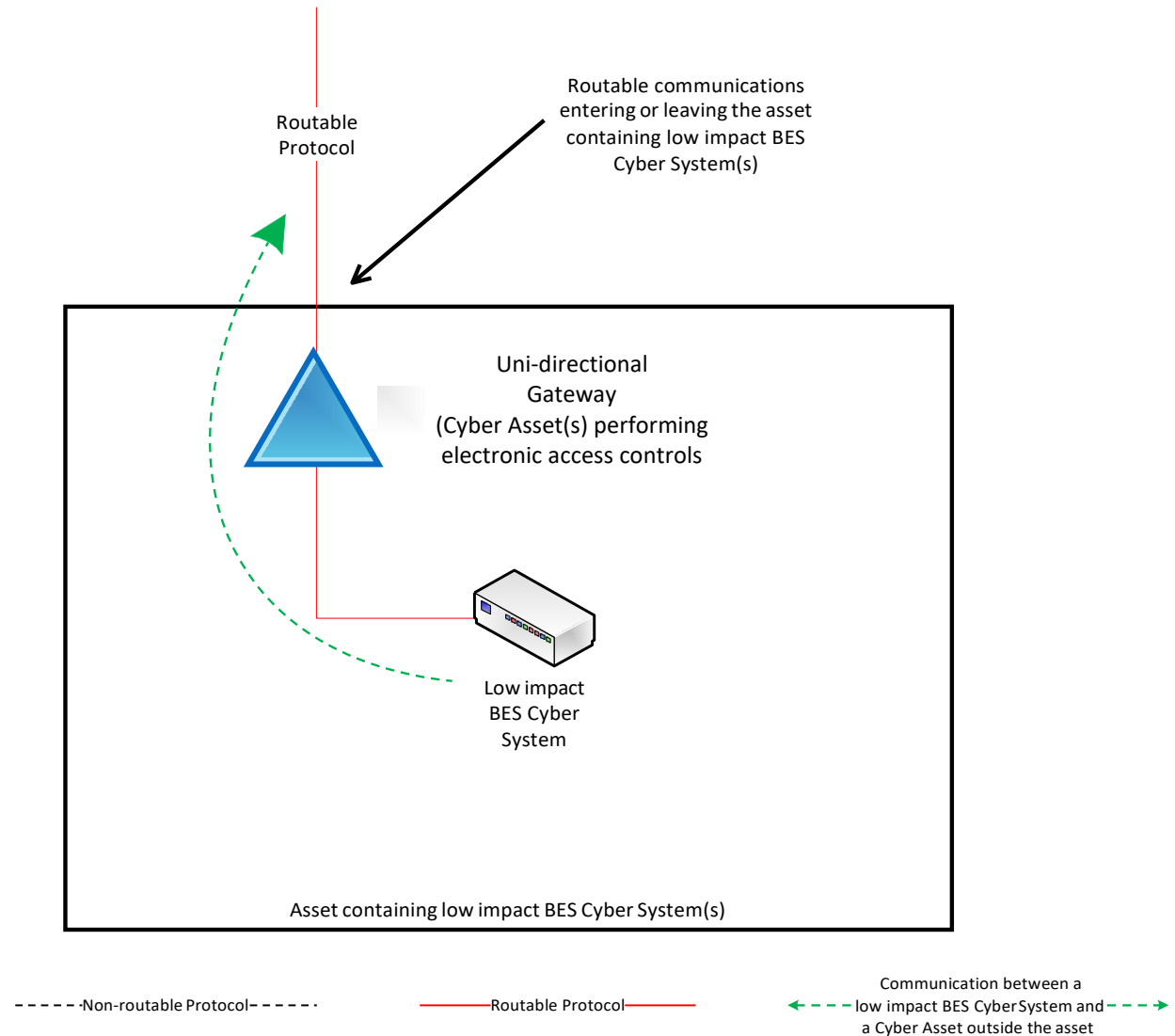


Reference Model 3

CIP-003-8 Supplemental Material

Reference Model 4 – Uni-directional Gateway

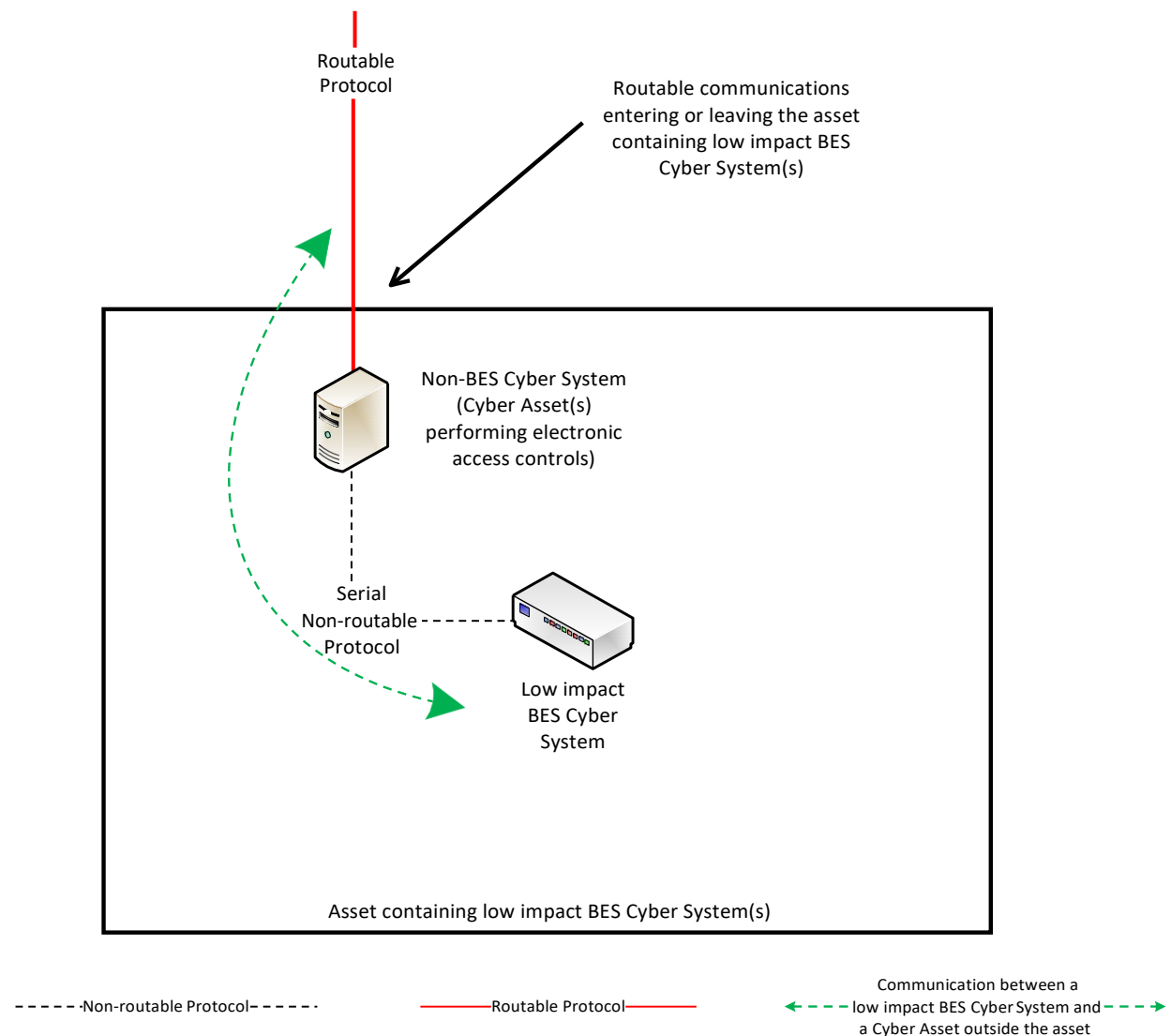
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way”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

*Reference Model 4*

CIP-003-8 Supplemental Material

Reference Model 5 – User Authentication

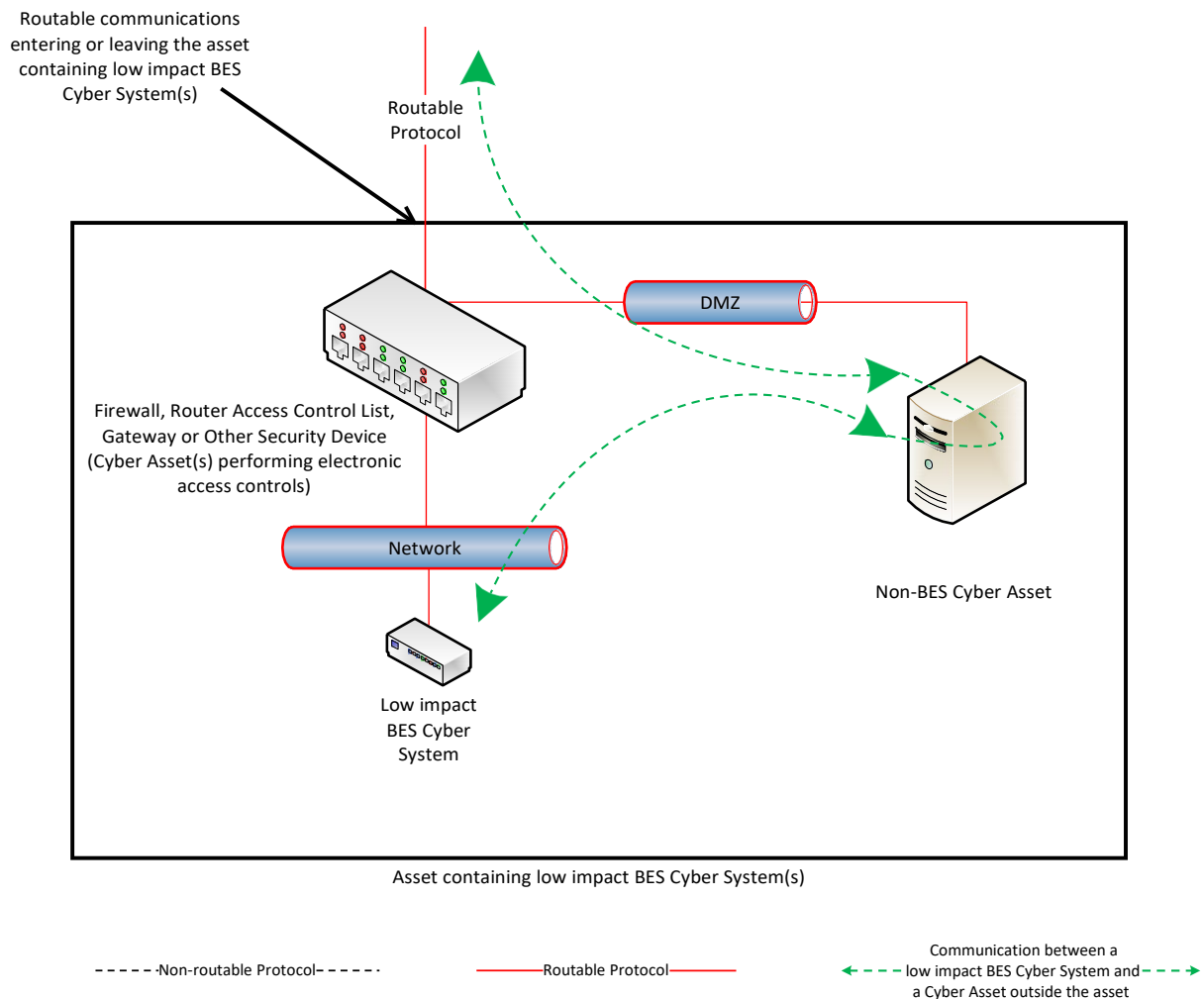
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber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

*Reference Model 5*

CIP-003-8 Supplemental Material

Reference Model 6 – Indirect Access

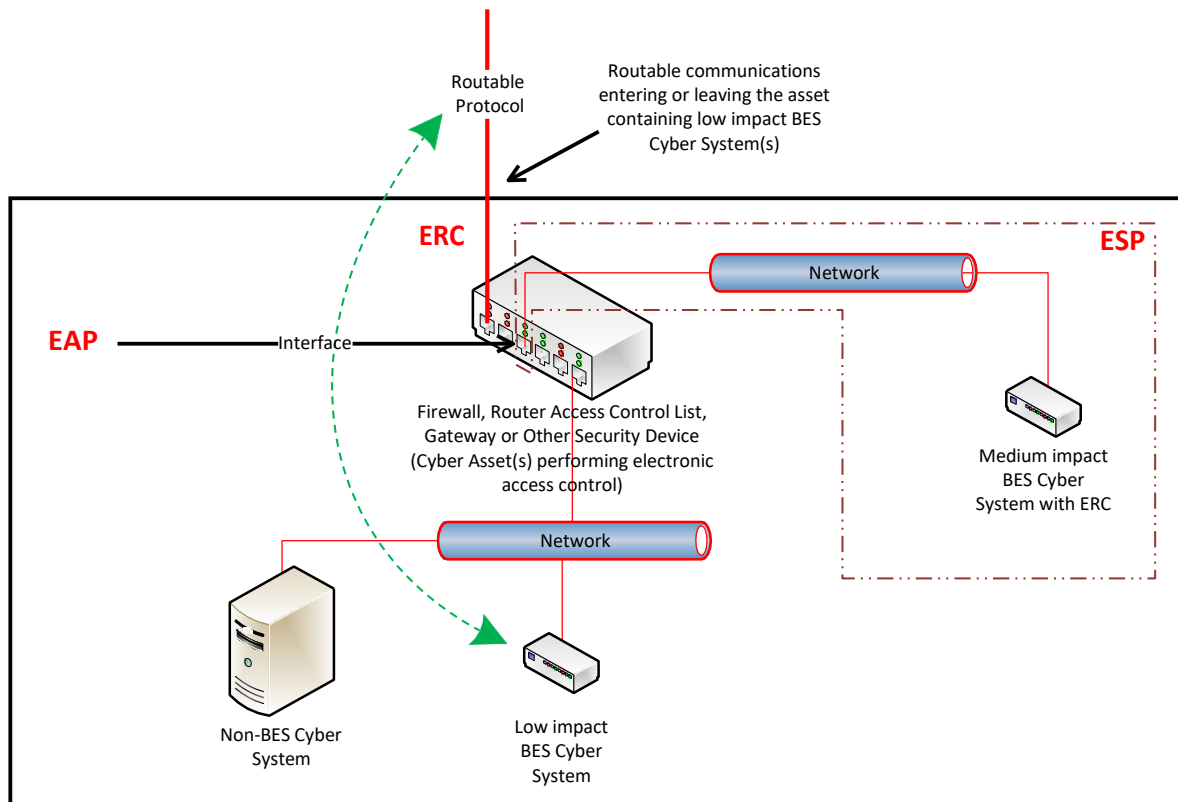
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.

*Reference Model 6*

CIP-003-8 Supplemental Material

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

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



Asset containing low impact BES Cyber System(s) and medium impact BES Cyber System(s)

----- Non-routable Protocol ----- ——— Routable Protocol ——— <----- Communication between a low impact BES Cyber System and a Cyber Asset outside the asset ----->

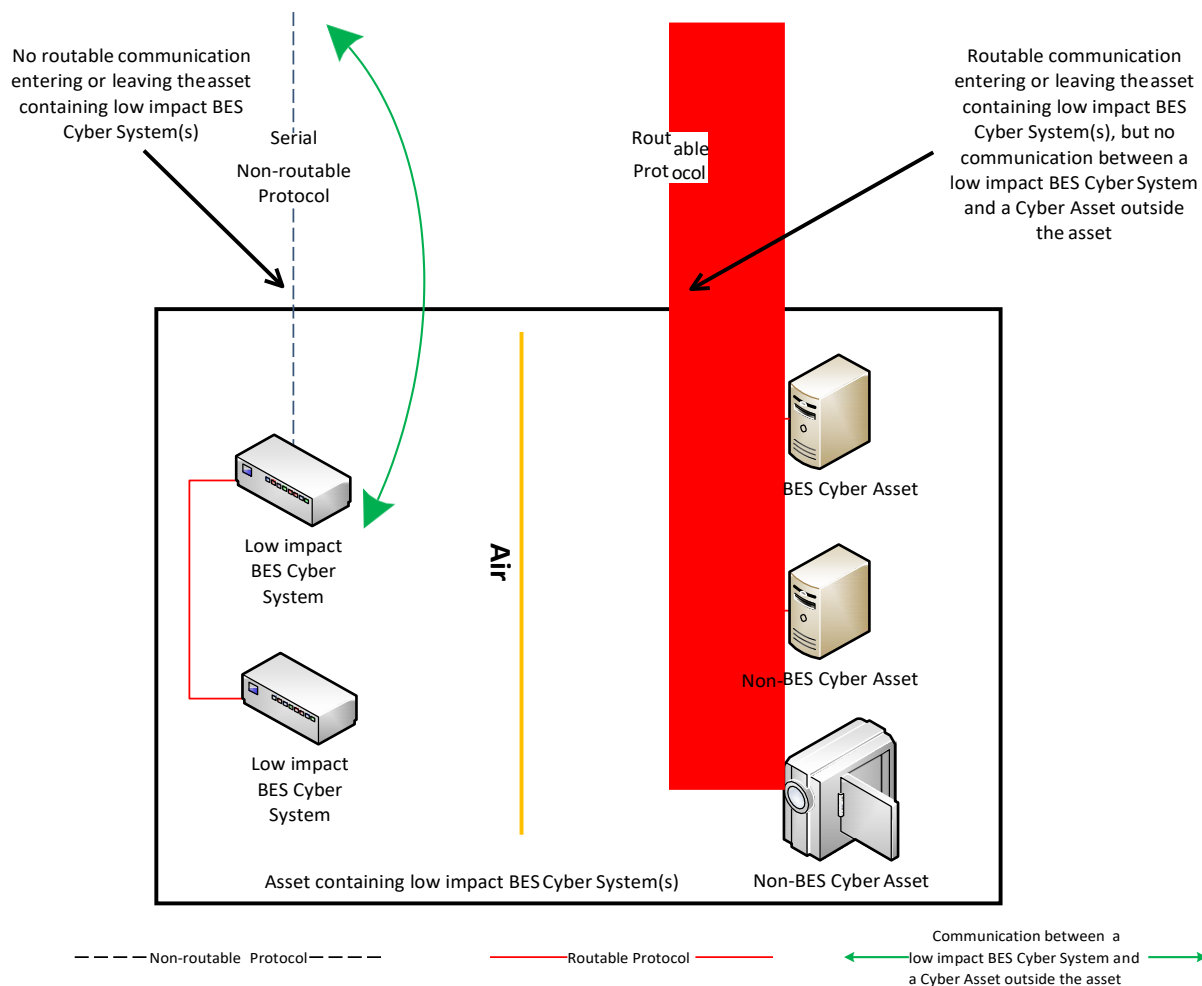
Reference Model 7

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

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

- 1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
- 2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
- 3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

CIP-003-8 Supplemental Material

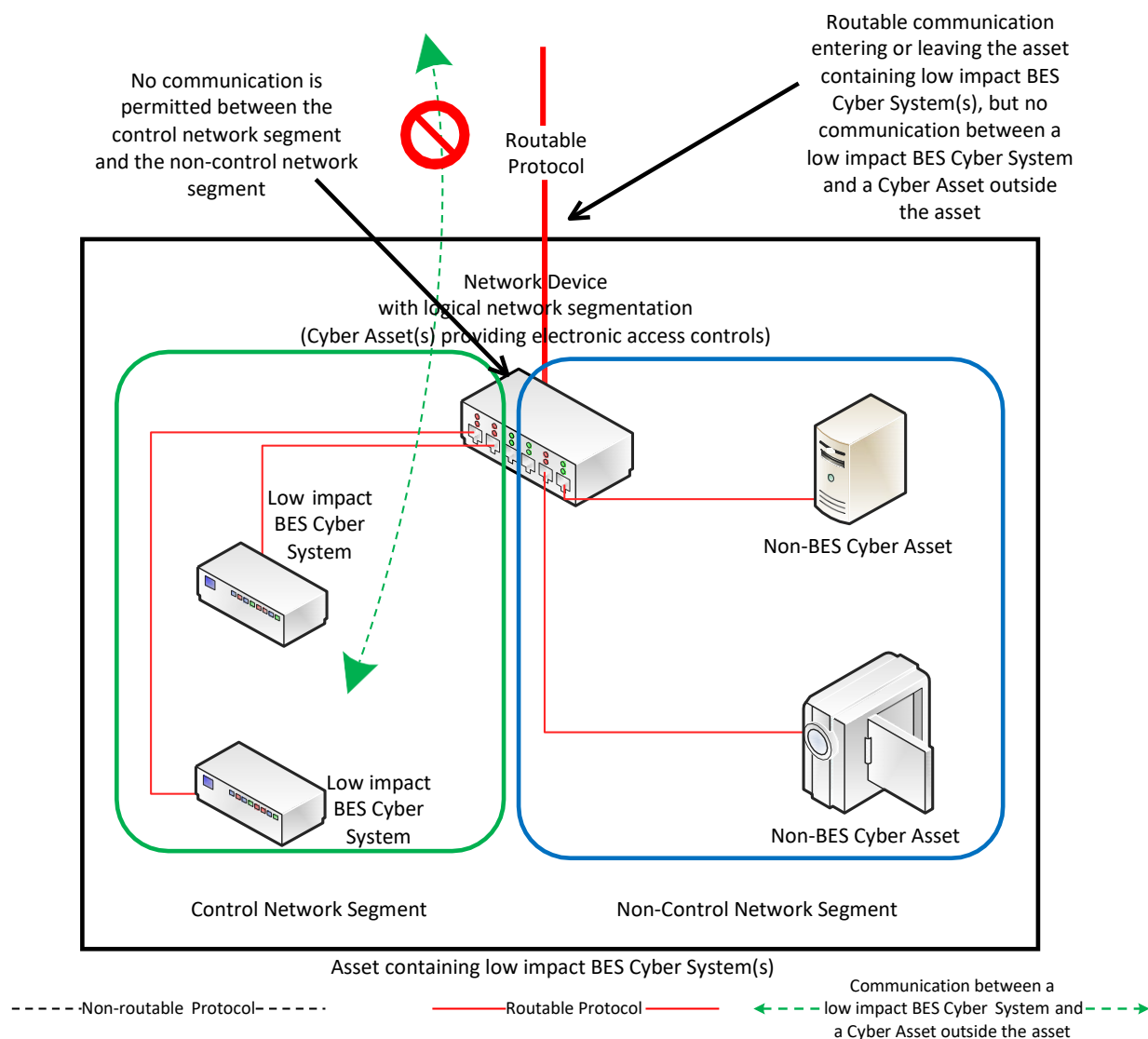


Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

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

CIP-003-8 Supplemental Material

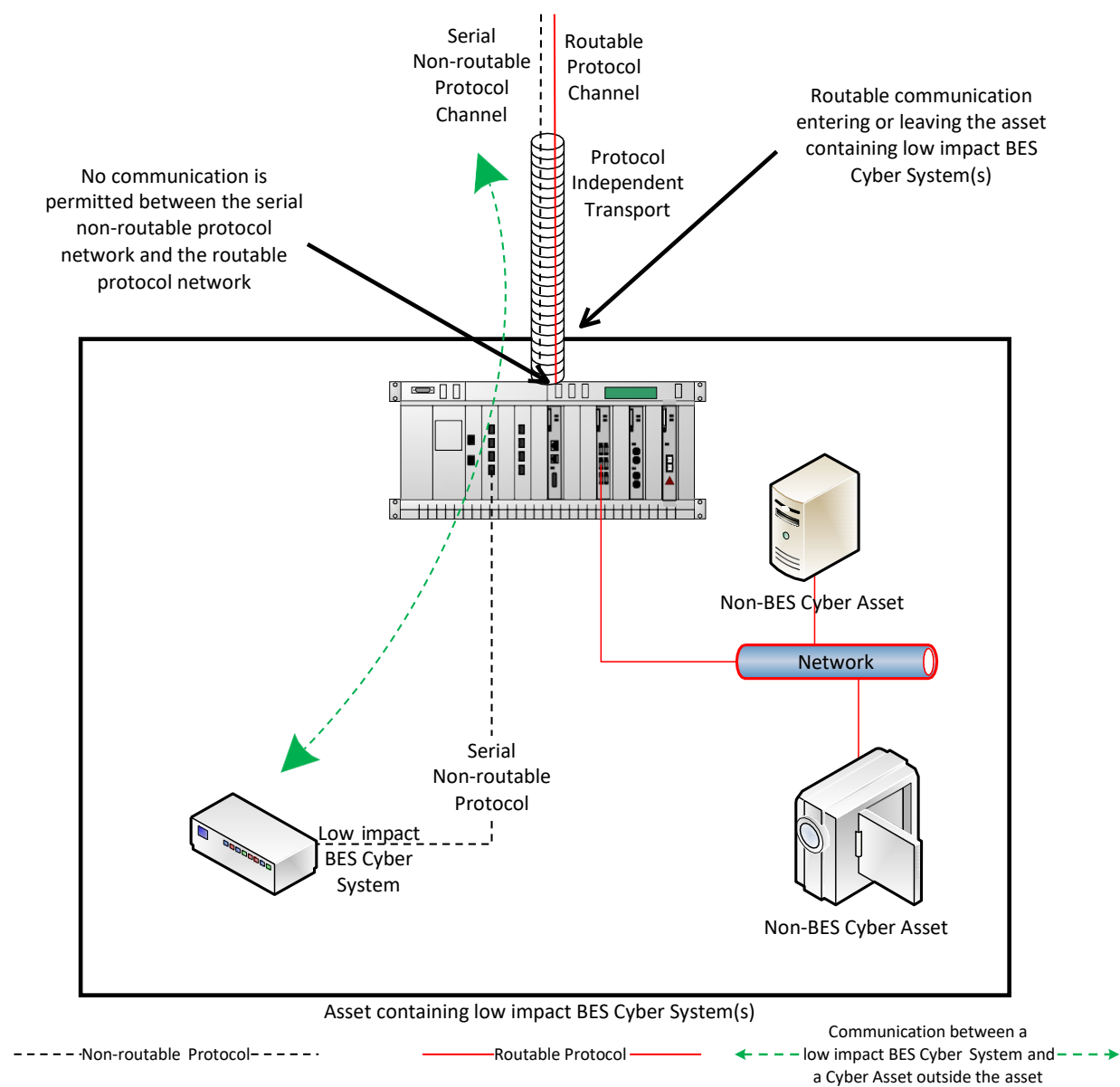


Reference Model 9

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

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

CIP-003-8 Supplemental Material



Reference Model 10

CIP-003-8 Supplemental Material

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to

CIP-003-8 Supplemental Material

disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

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

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

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

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

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

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

CIP-003-8 Supplemental Material

Malicious Code Risk Mitigation

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

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

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

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

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

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

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

CIP-003-8 Supplemental Material

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

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

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

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

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.¹ Procurement language may unify

¹<http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014>

CIP-003-8 Supplemental Material

the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

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

Requirement R2, Attachment 1, Section 5.3 - Removable Media

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

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System

CIP-003-8 Supplemental Material

network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

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

CIP-003-8 Supplemental Material

the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

CIP-003-8 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 BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

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

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

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

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "...the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6...to provide needed clarity to the definition

CIP-003-8 Supplemental Material

and eliminate ambiguity surrounding the term ‘direct’ as it is used in the proposed definition...within one year of the effective date of this Final Rule.”

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

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

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

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

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

Rationale for Requirement R3:

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

CIP-003-8 Supplemental Material

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

Rationale for Requirement R4:

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

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

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-6
3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**
 - 4.1.4. **Generator Owner**

4.1.5. 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 Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-6:

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

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

- 4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
- 4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
- 4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date*:

See Implementation Plan for Project 2016-03.

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

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

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

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

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

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

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

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

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

“Applicable Systems” Columns in Tables:

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

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

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> PCA Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> PCA 	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: <ul style="list-style-type: none"> PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ul style="list-style-type: none"> PCA 	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: <ul style="list-style-type: none"> • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: <ul style="list-style-type: none"> • PCA 	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

- R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-6 Table R2 –Remote Access Management*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M2.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ul style="list-style-type: none"> PCA 	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ul style="list-style-type: none"> PCA 	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

CIP-005-6 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none">• PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none">• PCA	<p>Require multi-factor authentication for all Interactive Remote Access sessions.</p>	<p>An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used.</p> <p>Examples of authenticators may include, but are not limited to,</p> <ul style="list-style-type: none">• Something the individual knows such as passwords or PINs. This does not include User ID;• Something the individual has such as tokens, digital certificates, or smart cards; or• Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

CIP-005-6 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.4	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none">• PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none">• PCA	<p>Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).</p>	<p>Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as:</p> <ul style="list-style-type: none">• Methods for accessing logged or monitoring information to determine active vendor remote access sessions;• Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or• Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

CIP-005-6 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.5	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none">• PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none">• PCA	<p>Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).</p>	<p>Examples of evidence may include, but are not limited to, documentation of the method(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as:</p> <ul style="list-style-type: none">• Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or• Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

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

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

Violation Severity Levels

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

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5).	Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

None.

CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)

Version History

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

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. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of ‘Associated Protected Cyber Assets’ that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the ‘high water mark’).

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

CIP-005-6 Supplemental Material

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the “high water mark”) where the term “Protected Cyber Assets” is used. The CIP Cyber Security Standards accomplish the “high water mark” by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as “Protected Cyber Assets” of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

CIP-005-6 Supplemental Material

between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

Rationale for R1:

The Electronic Security Perimeter (“ESP”) serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical “perimeter.”

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point (“EAP”).

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)

Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)

Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)

Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

CIP-005-6 Supplemental Material

Change Rationale: (Part 1.4)

Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)

Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

CIP-005-6 Supplemental Material

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-6
3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Reliability Coordinator**

4.1.6 Transmission Operator**4.1.7 Transmission Owner**

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

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

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

- 4.2.3.3** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.4** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
- 4.2.3.5** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates*:

See Implementation Plan for CIP-008-6.

6. Background:

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

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

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

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

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

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

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

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

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

“Applicable Systems” Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>One or more processes:</p> <p>1.2.1 That include criteria to evaluate and define attempts to compromise;</p> <p>1.2.2 To determine if an identified Cyber Security Incident is:</p> <ul style="list-style-type: none"> A Reportable Cyber Security Incident; or An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and <p>1.2.3 To provide notification per Requirement R4.</p>	<p>Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.</p>

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

- R2.** Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].
- M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>Test each Cyber Security Incident response plan(s) at least once every 15 calendar months:</p> <ul style="list-style-type: none"> By responding to an actual Reportable Cyber Security Incident; With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or With an operational exercise of a Reportable Cyber Security Incident. 	<p>Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.</p>

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.</p>	<p>Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.</p>	<p>An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column.</p>

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

- R3.** Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*.

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:</p> <p>3.1.1. Document any lessons learned or document the absence of any lessons learned;</p> <p>3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and</p> <p>3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.</p>	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none">• EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none">• Emails;• USPS or other mail service;• Electronic distribution system; or• Training sign-in sheets.

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

- R4.** Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),¹ or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M4.** Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents*.

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> EACMS 	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: <ul style="list-style-type: none"> 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted. 	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

¹ The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines:</p> <ul style="list-style-type: none"> One hour after the determination of a Reportable Cyber Security Incident. By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part. 	<p>Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.</p>
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.</p>	<p>Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.</p>

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

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning	Lower	N/A	N/A	<p>The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3)</p> <p>OR</p> <p>The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)</p> <p>OR</p> <p>The Responsible Entity has developed a Cyber</p>	<p>The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1)</p> <p>OR</p> <p>The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in</p>

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2)</p> <p>OR</p> <p>The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (1.2)</p>	the “Applicable Systems” column for Part 1.2. (1.2)
R2	Operations Planning Real-time Operations	Lower	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (2.1)	<p>The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (2.1)</p> <p>OR</p>

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.2 occurs. (2.2)	The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.3. (2.3)
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response to a Reportable Cyber Security Incident. (3.1.3)	<p>Security Incident. (3.1.2)</p> <p>OR</p> <p>The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)</p> <p>OR</p> <p>The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days</p>	<p>Security Incident. (3.1.1)</p> <p>OR</p> <p>The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2)</p> <p>OR</p> <p>The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity</p>	Security Incident. (3.1.1)

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2)</p> <ul style="list-style-type: none"> • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. 	<p>determines would impact the ability to execute the plan: (3.2)</p> <ul style="list-style-type: none"> • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. 	
R4	Operations Assessment	Lower	<p>The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the</p>	<p>The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column. (R4)</p>	<p>The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2)</p> <p>OR</p>	<p>The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)</p>

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>timelines pursuant to Part 4.2. (4.2)</p> <p>OR</p> <p>The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3)</p> <p>OR</p> <p>The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a</p>		<p>The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)</p>	

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-008-6 - Cyber Security — Incident Reporting and Response Planning

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

CIP-008-6 - Cyber Security — Incident Reporting and Response Planning

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	2/6/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments
2. **Number:** CIP-010-3
3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**

4.1.4. Generator Owner

4.1.5. 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 Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

- 4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
- 4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
- 4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. **Effective Date*:**

See Implementation Plan for Project 2016-03.

6. **Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

“Applicable Systems” Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Develop a baseline configuration, individually or by group, which shall include the following items:</p> <ol style="list-style-type: none"> 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied. 	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Authorize and document changes that deviate from the existing baseline configuration.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.</p>	<p>An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.</p>
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>For a change that deviates from the existing baseline configuration:</p> <ol style="list-style-type: none"> 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification. 	<p>An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber Systems	<p>Where technically feasible, for each change that deviates from the existing baseline configuration:</p> <p>1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and</p> <p>1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.</p>	<p>An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.6	<p>High Impact BES Cyber Systems</p> <p>Medium Impact BES Cyber Systems</p> <p>Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.</p>	<p>Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:</p> <p>1.6.1. Verify the identity of the software source; and</p> <p>1.6.2. Verify the integrity of the software obtained from the software source.</p>	<p>An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.</p>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R2 – Configuration Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

- R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*
- M3.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems	<p>Where technically feasible, at least once every 36 calendar months:</p> <p>3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and</p> <p>3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.</p>	<p>An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PCA 	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

- R4.** Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*
- M4.** Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The British Columbia Utilities Commission.

- 1.2. Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the 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 applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	<p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)</p> <p>OR</p> <p>The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)</p>	<p>The Responsible Entity has not documented or implemented any configuration change management process(es). (R1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)</p> <p>OR</p> <p>The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>OR</p> <p>The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)</p> <p>OR</p> <p>The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1)</p> <p>OR</p> <p>The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)</p> <p>OR</p> <p>The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1)</p> <p>OR</p> <p>The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>OR</p> <p>The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)</p>
R2.	N/A	N/A	N/A	<p>The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)</p>
R3.	<p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has</p>	<p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has</p>	<p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has</p>	<p>The Responsible Entity has not implemented any vulnerability assessment processes for one of its</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>performed a vulnerability assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>applicable BES Cyber Systems. (R3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>applicable BES Cyber Systems.(3.2)</p> <p>OR</p> <p>The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	<p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections</p>	<p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software</p>	<p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software</p>	<p>The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)</p>

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)</p>	<p>vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,</p>	<p>vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,</p>	

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

- 1.1. Transient Cyber Asset Management:** Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.
- 1.2. Transient Cyber Asset Authorization:** For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:
 - 1.2.1.** Users, either individually or by group or role;
 - 1.2.2.** Locations, either individually or by group; and
 - 1.2.3.** Uses, which shall be limited to what is necessary to perform business functions.
- 1.3. Software Vulnerability Mitigation:** Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):
 - Security patching, including manual or managed updates;
 - Live operating system and software executable only from read-only media;
 - System hardening; or
 - Other method(s) to mitigate software vulnerabilities.
- 1.4. Introduction of Malicious Code Mitigation:** Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):
 - Antivirus software, including manual or managed updates of signatures or patterns;
 - Application whitelisting; or
 - Other method(s) to mitigate the introduction of malicious code.
- 1.5. Unauthorized Use Mitigation:** Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

- 3.1.1.** Users, either individually or by group or role; and
- 3.1.2.** Locations, either individually or by group.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

- 3.2.** Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:
- 3.2.1.** Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and
 - 3.2.2.** Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset’s baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset’s baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

Guidelines and Technical Basis

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Guidelines and Technical Basis

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful “Watering Hole” or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

Guidelines and Technical Basis

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Guidelines and Technical Basis

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

Guidelines and Technical Basis

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

Guidelines and Technical Basis

connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

- 1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.
- 1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.
- 1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,

Guidelines and Technical Basis

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Guidelines and Technical Basis

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that

Guidelines and Technical Basis

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.¹ Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support.

¹ <http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014>

Guidelines and Technical Basis

Entities should consider the “General Cybersecurity Procurement Language” and “The Supplier’s Life Cycle Security Program” when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party’s security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Guidelines and Technical Basis

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

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

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the

Guidelines and Technical Basis

SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

A. Introduction

1. **Title:** Cyber Security - Supply Chain Risk Management
2. **Number:** CIP-013-1
3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. Balancing Authority
 - 4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.3. Generator Operator
 - 4.1.4. Generator Owner
 - 4.1.5. Reliability Coordinator
 - 4.1.6. Transmission Operator
 - 4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

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

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date*: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and

1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

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

CIP-013-1 – Cyber Security - Supply Chain Risk Management

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The British Columbia Utilities Commission.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the 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 Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	<p>The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.</p> <p>OR</p> <p>The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.</p>

CIP-013-1 – Cyber Security - Supply Chain Risk Management

R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within

CIP-013-1 – Cyber Security - Supply Chain Risk Management

	so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	18 calendar months of the previous review as specified in the Requirement.
--	---	---	---	--

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	

Supplemental Material

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

- (1) Software integrity and authenticity;
- (2) Vendor remote access;
- (3) Information system planning; and
- (4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks.

Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the

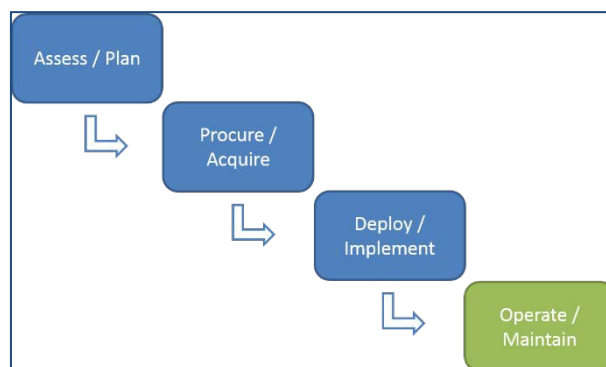
Supplemental Material

awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Supplemental Material

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

A. Introduction

1. **Title:** Reliability Coordination – Monitoring and Analysis
2. **Number:** IRO-002-6
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]*

IRO-002-6 - Reliability Coordination - Monitoring and Analysis

- 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

IRO-002-6 - Reliability Coordination - Monitoring and Analysis

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>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;</p> <p>OR</p> <p>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.</p>	<p>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;</p> <p>OR</p> <p>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.</p>	<p>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;</p> <p>OR</p> <p>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.</p>	<p>capabilities specified in Requirement R2 for redundant functionality, but did so more than 180 calendar days since the previous test;</p> <p>OR</p> <p>The Reliability Coordinator did not test its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality;</p> <p>OR</p> <p>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.</p>
R4.	N/A	N/A	N/A	The Reliability Coordinator failed to provide its System Operator with the authority to approve planned outages and

IRO-002-6 - Reliability Coordination - Monitoring and Analysis

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

IRO-002-6 - Reliability Coordination - Monitoring and Analysis

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				information systems, over a redundant infrastructure.

D. Regional Variance

A. Regional Variance for the Western Electricity Coordinating Council Region

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

Purpose

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

Applicability

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

Requirements and Measures

- D.A.7.** Each Reliability Coordinator shall, in coordination with other Reliability Coordinators, develop a common Interconnection-wide methodology to determine the modeling and monitoring of BES and non-BES Elements that are internal and external to its Reliability Coordinator Area, necessary for providing operational awareness of the impacts on Bulk Electric System Facilities within its Reliability Coordinator Area, including at a minimum: *([Violation Risk Factor: High] [Time Horizon: Operations Planning])*
- D.A.7.1.** A method for development, maintenance, and periodic review of a Western Interconnection-wide reference model to serve as the baseline from which Reliability Coordinator's operational models are derived;
 - D.A.7.2.** The impacts of Inter-area oscillations;
 - D.A.7.3.** A method to determine Contingencies included in analyses and assessments;
 - D.A.7.4.** A method to determine Remedial Action Schemes included in analyses and assessments;
 - D.A.7.5.** A method to determine forecast data included in analyses and assessments; and
 - D.A.7.6.** A method for the validation and periodic review of the Reliability Coordinator's operational model for steady state and dynamic/oscillatory system response.
- M.DA.7.** Each Reliability Coordinator will have evidence that it developed a common Western Interconnection-wide methodology, addressing modeling and

IRO-002-6 - Reliability Coordination - Monitoring and Analysis

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

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

MDA8. Each Reliability Coordinator will have evidence that it uses the methodology developed in D.A.7., as required in D.A.8. above.

Compliance

Evidence Retention:

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

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

E. Associated Documents

The Implementation Plan and other project documents can be found on the [project page](#).

IRO-002-6 - Reliability Coordination - Monitoring and Analysis

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	

IRO-002-6 - Reliability Coordination - Monitoring and Analysis

6	May 9, 2019	Adopted by the NERC Board of Trustees	WECC Regional Variance
6	July 11, 2019	FERC Letter Order approved IRO-002- 6. Docket No. RD19-6-000	

Supplemental Material

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

Supplemental Material

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:** Qualified Path Unscheduled Flow (USF) Relief
2. **Number:** IRO-006-WECC-3
3. **Purpose:** To mitigate flows on Qualified Paths to reliable levels during Real-time operations.
4. **Applicability**
 - 4.1. Reliability Coordinator
 - 4.2. Balancing Authority
5. **Effective Date*:** The first day of the second quarter following applicable regulatory approval. See Implementation Plan.

B. Requirements and Measures

- R1.** Each Reliability Coordinator receiving a request for Curtailments for unscheduled flow transmission relief on a Qualified Path within its Reliability Coordinator Area shall either approve or deny that request within five minutes of receipt. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*
- M1.** Each Reliability Coordinator receiving a request for Curtailments for unscheduled flow transmission relief on a Qualified Path within its Reliability Coordinator Area, per requirement R1, will have evidence that it approved or denied that request within five minutes of receipt. Evidence may include, but is not limited to documentation of either an active or passive approval.
- R2.** Each Balancing Authority receiving an approved request for unscheduled flow transmission relief on a Qualified Path per Requirement R1, shall perform any of the following actions to meet that request: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*
- Approve curtailment requests to the schedules as submitted
 - Implement alternative actions
- M2.** Each Balancing Authority receiving an approved request for unscheduled flow transmission relief on a Qualified Path per Requirement R1, will have

evidence that it performed the actions allowed in Requirement R2, to meet that request.

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 Reliability Coordinator and each Balancing Authority shall keep data or evidence to show compliance with Requirements R1 and R2 for three calendar years or for the duration of any Compliance Enforcement Authority investigation, whichever is longer.
- If the Reliability Coordinator or Balancing Authority is found noncompliant, it shall keep information related to the noncompliance until found compliant or for the duration specified above, whichever is longer.

1.3. Compliance Monitoring and Enforcement Program

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

IRO-006-WECC-3 – Qualified Path Unscheduled Flow Relief

Violation Severity Levels

	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations	Medium	Not Applicable	Not Applicable	Not Applicable	There shall be a Severe level of noncompliance if there is one instance during a calendar month in which the Reliability Coordinator approved (actively or passively) or denied a request for unscheduled flow transmission relief on a Qualified Path greater than five minutes after receipt that request.
R2	Real-time Operations	Medium	There shall be a Lower Level of noncompliance if there is less than 100% relief requirement provided but greater than or equal to 90% relief requirement provided or the relief requirement was less	There shall be a Moderate Level of noncompliance if there is less than 90% relief requirement provided but greater than or equal to 75% relief requirement provided.	There shall be a High Level of noncompliance if there is less than 75% relief requirement provided but greater than or equal to 60% relief requirement provided.	There shall be a Severe Level of noncompliance if there is less than 60% relief requirement provided.

IRO-006-WECC-3 – Qualified Path Unscheduled Flow Relief

	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			than 5 MW and was not fully provided.			

D. Regional Variances

None.

E. Associated Documents

Western Interconnection Unscheduled Flow Mitigation Plan (WIUFMP).

IRO-006-WECC-3 – Qualified Path Unscheduled Flow Relief**Version History**

Version	Date	Action	Change Tracking
1	April 16, 2008	Permanent Replacement Standard for IRO-STD-006-0	
1	February 10, 2009	Adopted by NERC Board of Trustees	
1	March 17, 2011	FERC Order 746 issued by FERC approving IRO-006-WECC-1 (FERC approval effective on May 24, 2011)	
1	May 2, 2012	Updated the requirements to R1. and R2. instead of R.1. and R1.2.	
1	July 1, 2011	Effective Date	No Change
2	February 7, 2013	Adopted by NERC Board of Trustees	
2	May 13, 2014	FERC letter order issued approving IRO-006-WECC-2 (effective July 1, 2014).	
3	February 7, 2019	Adopted by NERC Board of Trustees	Five-year review. Defined term “Qualified Transfer Path” changed to “Qualified Path” as included in the Western Interconnection Unscheduled Flow Mitigation Plan, as approved by FERC. The following defined terms were retired: 1) Qualified Transfer Path, 2) Contributing Schedule, 3) Qualified Controllable Device, 4) Relief Requirement, 5) Transfer Distribution Factor, and 6) Qualified Transfer Path Curtailment Event.
3	May 10, 2019	FERC letter order issued approving IRO-006-WECC-3. Docket No. RD19-4-000.	

IRO-006-WECC-3 – Qualified Path Unscheduled Flow Relief
