

Standard Development Timeline

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

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11 – June 24, 2021
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization
2. **Number:** CIP-002-7
3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the BES. Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7:

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

- 4.2.3.2. Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).
- 4.2.3.3. Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.
- 4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modification to CIP Standards Implementation Plan”.

B. Requirements and Measures

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

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

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

C. Compliance

1. Compliance Monitoring Process:

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

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

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

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

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

Violation Severity Levels

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>been categorized or have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, five or fewer identified BCS or independently identified SCI have not been categorized or have been incorrectly categorized at a lower category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, five percent or fewer high or medium BCS have not been identified;</p> <p>OR</p>	<p>than five percent but less than or equal to 10 percent of identified BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BCS or independently</p>	<p>less than or equal to 15 percent of identified BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high or medium impact and BCA, more than 10 but less than or equal to 15 identified BCA have not been categorized or have been incorrectly categorized at a lower category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, more than 10 percent but less than or equal to 15</p>	<p>have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than 15 identified BCS or independently identified SCI have not been categorized or have been incorrectly categorized at a lower category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, more than 15 percent of high or medium impact BCS or independently identified SCI, have not been identified;</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, five or fewer high or medium BCS or independently identified SCI, have not been identified.	identified SCI, more than five percent but less than or equal to 10 percent high or medium BCS or independently identified SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than five but less than or equal to 10 high or medium BCS or independently identified SCI, have not been identified.	percent high or medium BCS or independently identified SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than 10 but less than or equal to 15 high or medium BCS or independently identified SCI, have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than 15 high or medium impact BCS or independently identified SCI, have not been identified.
R2	Operations Planning	Lower	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Requirement R2 Part 2.2)	calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Requirement R2 Part 2.2)	calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Requirement R2 Part 2.2)	(Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Requirement R2 Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation plan”.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. 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.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6		Criteria 2.12 Modifications Withdrawn	
7		Virtualization modifications.	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

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

1. High Impact Rating

Each BCS used by and located at any of the following:

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

2. Medium Impact Rating

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

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are:
 - Each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection; or
 - Any SCI (which must be included in a shared BCS) supporting one or more BCS that together could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
 - 2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.
-

- 2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
- 2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
- 2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

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

- 2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.
- 2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to

operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

- 2.10.** Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.
- 2.11.** Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.
- 2.12.** Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating, above.
- 2.13.** Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

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

- 3.1.** Control Centers and backup Control Centers.
- 3.2.** Transmission stations and substations.
- 3.3.** Generation resources.
- 3.4.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.
- 3.5.** RAS that support the reliable operation of the BES.
- 3.6.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.