

**Exhibit A**

**Proposed Reliability Standards**

**Reliability Standard CIP-003-6 Clean and Redline**

## A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-6
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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
    - 4.1.3 **Generator Operator**
    - 4.1.4 **Generator Owner**
    - 4.1.5 **Interchange Coordinator or Interchange Authority**
    - 4.1.6 **Reliability Coordinator**

**4.1.7 Transmission Operator**

**4.1.8 Transmission Owner**

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

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-003-6:

**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 (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-003-6.

**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 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 for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and
    - 1.2.4.** Cyber Security Incident response
- 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]*

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:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

#### 1.4. Additional Compliance Information:

None

**2. Table of Compliance Elements**

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R1</b>	<b>Operations Planning</b>	<b>Medium</b>	<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>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR 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 four topics required by R1. (R1.2) OR 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	the previous approval. (R1.1) OR 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 four topics required by R1. (R1.2) OR 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	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR 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 not complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR 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 any of the four topics required by R1. (R1.2) OR 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)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>required by Requirement R1 within 15 calendar months but did not 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 not complete this</p>	<p>required by Requirement R1 within 16 calendar months but did not 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</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 not complete this approval in less than or equal to 18 calendar months of the previous approval. (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 18 calendar months of the previous approval. (R1.2)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
<b>R2</b>	<b>Operations Planning</b>	<b>Lower</b>	<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 CIP-003-6, 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</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 CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more incident response plans</p>	<p>The Responsible Entity documented one or more Cyber Security Incident response plans 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 CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented the determination of</p>	<p>The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2,</p>	<p>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 according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2)</p> <p>(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</p>	<p>whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)</p> <p>OR</p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2)	<p>whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4.</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 physical security controls according to CIP-003-6,</p>	<p>The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)</p> <p>OR</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 CIP-003-6,</p>	



R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 2. (R2)  OR  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 CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)	Requirement R2, Attachment 1, Section 2. (R2)	
<b>R3</b>	<b>Operations Planning</b>	<b>Medium</b>	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager	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	The Responsible Entity has not identified, by name, a CIP Senior Manager.  OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R3)	within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	document this change in less than 60 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 60 calendar days of the change. (R3)
<b>R4</b>	<b>Operations Planning</b>	<b>Lower</b>	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4)  OR The Responsible Entity has identified a delegate by name, title, date of delegation, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						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	<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3	12/16/09	<p>Updated Version Number from -2 to -3</p> <p>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.</p>	
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.
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

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/2015	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.

## CIP-003-6 - 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 Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

**Section 3. Electronic Access Controls:** Each Responsible Entity shall:

- 3.1** For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and
- 3.2** Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, 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 Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;
- 4.3** Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- 4.4** Incident handling for Cyber Security Incidents;
- 4.5** 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

- 4.6** 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.

## CIP-003-6 - 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, if any, containing a LEAP.

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

- Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and 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 Sector Information Sharing and Analysis Center (ES-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.

## 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-003-6, 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-003-6, 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 four 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-003-6, 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 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 should 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
- 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

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:**

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse

or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

### **Requirement R2, Attachment 1**

As noted, Attachment 1 contains the sections that must be 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. Guidance for each of the four 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 Responsible Entity is not 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) low impact BES Cyber Systems at assets containing low impact BES Cyber System(s) and (2) LEAPs, if any. If the LEAP is located within the BES asset and inherits the same controls outlined in Section 2, this can 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 in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems, the low impact BES Cyber Systems themselves, or LEAPs, if any. The Responsible Entity may use one or a combination of 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. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems, including LEAPs. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to 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 monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

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

Section 3 requires the establishment of boundary protections for low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term “electronic access control” is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude “point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems,” such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases “direct user-initiated interactive access or a direct device-to-device connection

to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.” The intent of “direct” in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for “device-to-device connection,” LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems “behind” it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a “pass-through” of the data flow communication, then that “pass-through” data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and

other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a “protocol break” so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.
- 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.

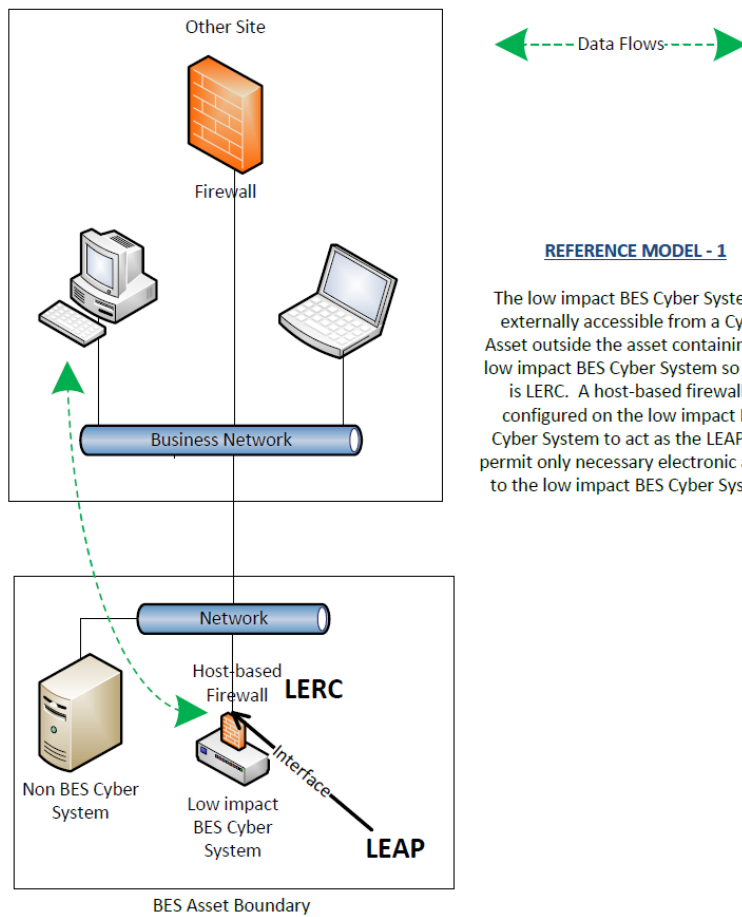
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

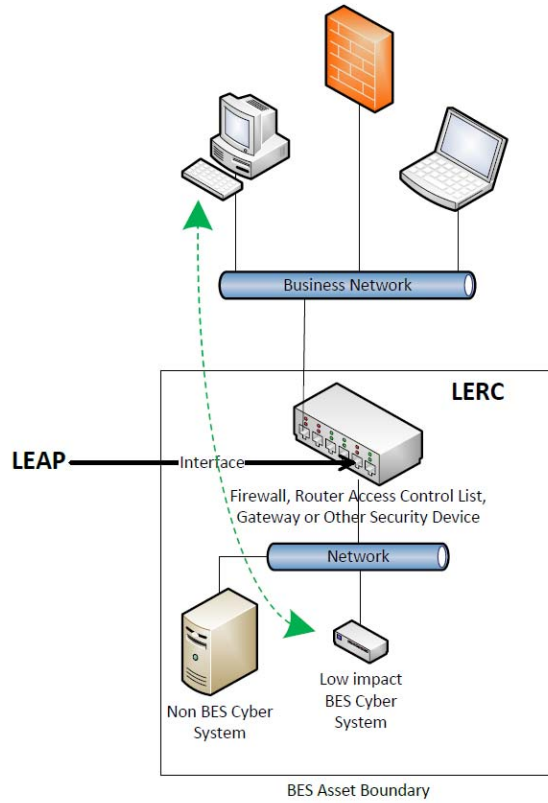
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a 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.
- In Reference Model 5, using just 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 and the business network would not meet the intent of “controlling” inbound and



outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

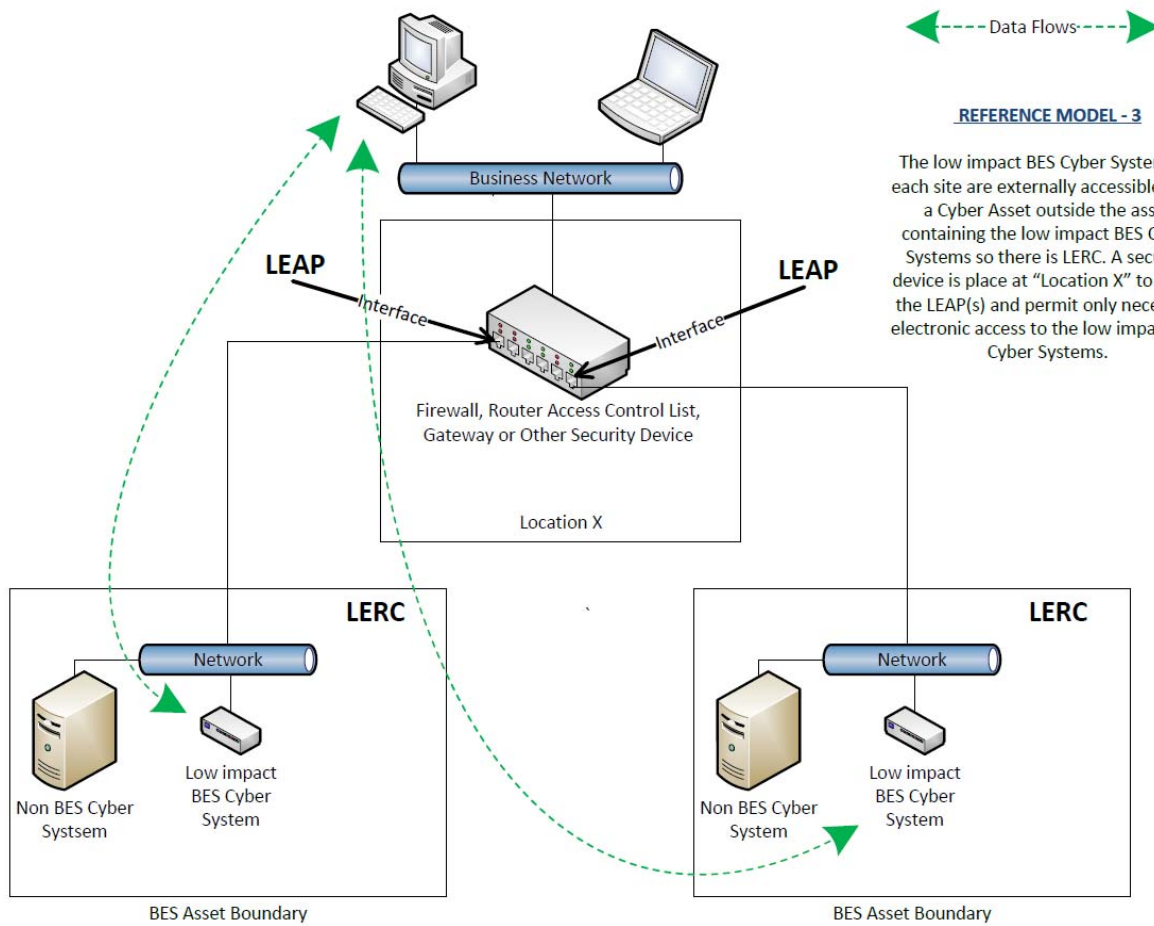
The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.





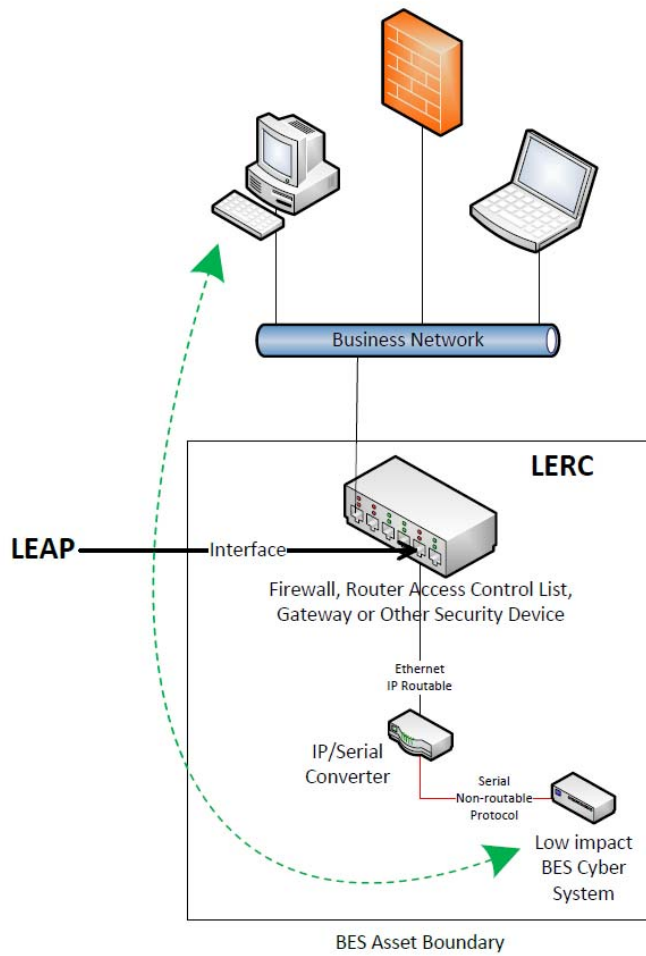
**REFERENCE MODEL - 2**

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.



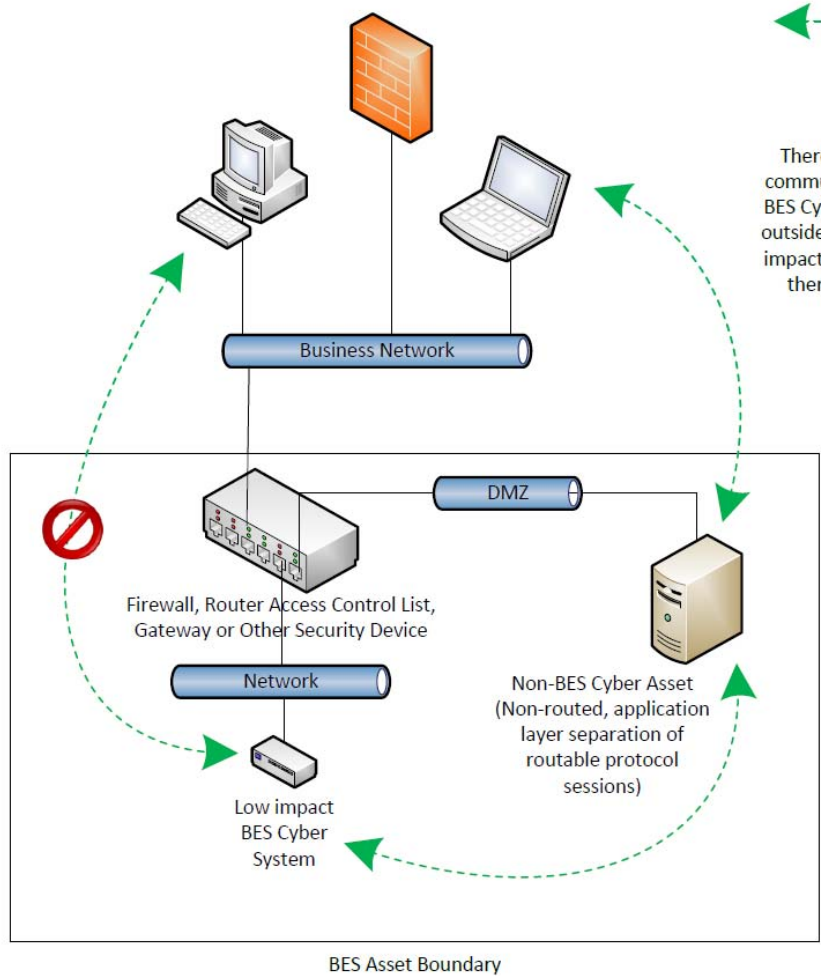
**REFERENCE MODEL - 3**

The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is placed at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.



**REFERENCE MODEL - 4**

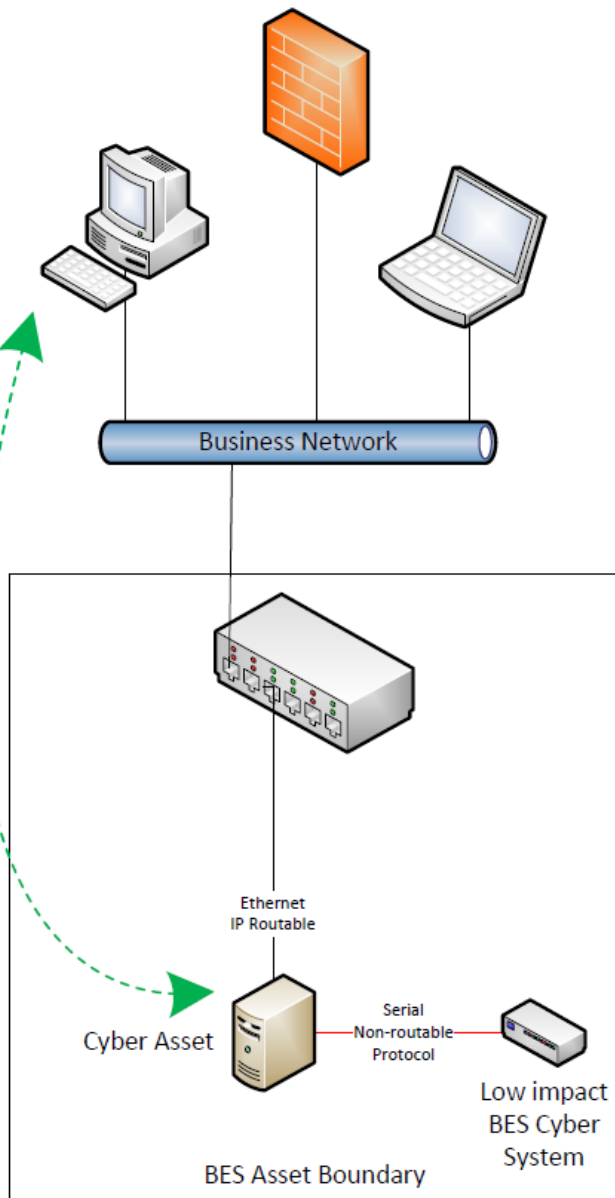
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.



←--- Data Flows ---→

**REFERENCE MODEL - 5**

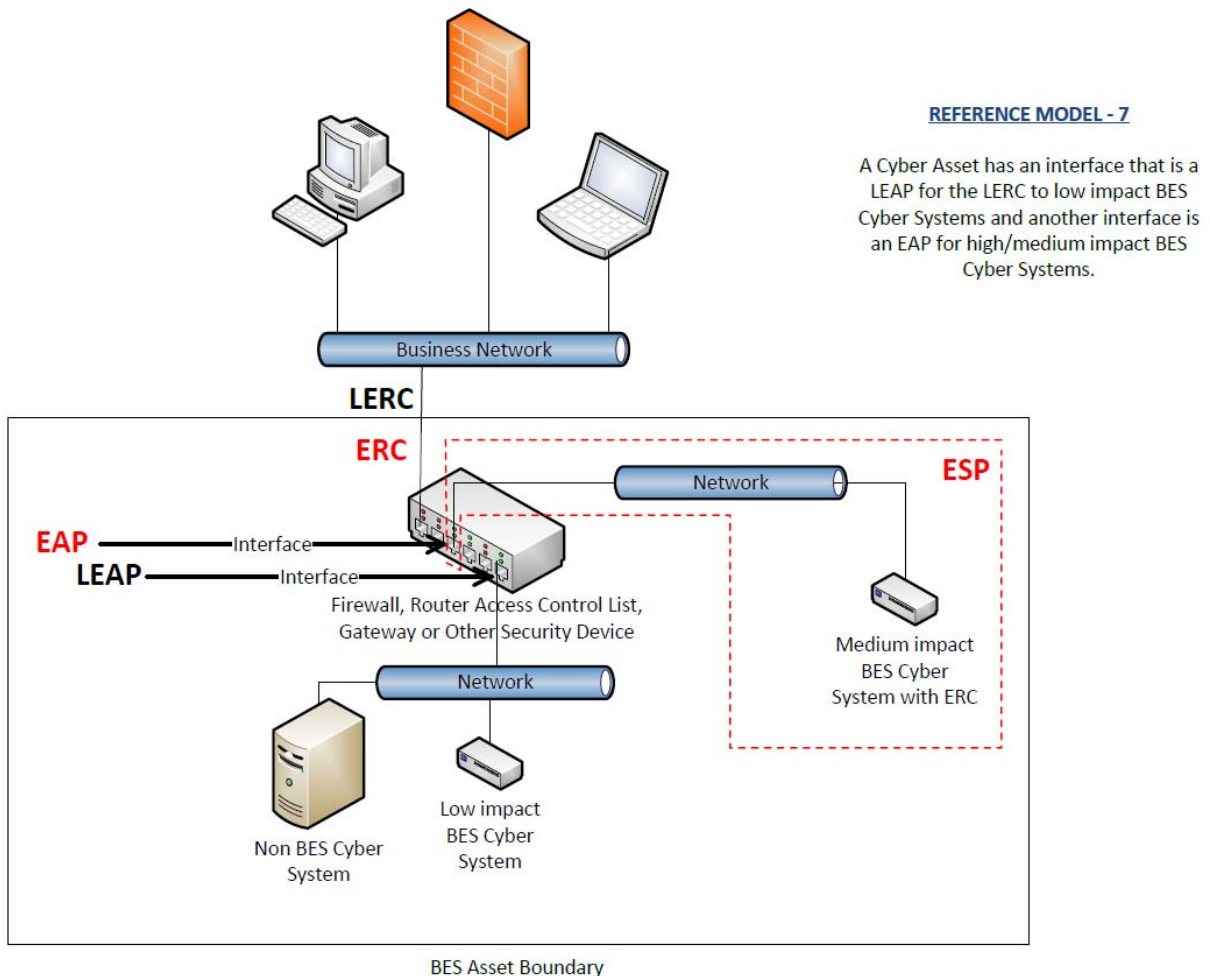
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.



← Data Flows →

**REFERENCE MODEL - 6**

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



**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 Systems, 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 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 R3:**

The intent of CIP-003-6, 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-003-6, 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 the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.



**Rationale:**

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

**Rationale for 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 Systems. The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. 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 Systems. However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

**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.

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 — Security Management Controls
2. **Number:** CIP-003-~~56~~
3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the ~~BES~~ Bulk Electric System (BES).
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

**4.2.1.2** Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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-~~56~~:

**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. ~~5.~~ Effective Dates:**

~~1. **24 Months Minimum**— CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-003-6.

**6. Background:**

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

The term *policy* refers to as the Version 5 CIP Cyber Security Standards, 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 SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:-~~

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

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

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

Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security 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 ~~and~~, medium, and low impact BES Cyber Systems. For example, a single ~~training~~cyber security awareness program could meet the requirements ~~for training personnel~~ across multiple BES Cyber Systems.

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

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

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

## B. Requirements and Measures

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

**1.1** For its high impact and medium impact BES Cyber Systems, if any:

- 1.1.1.** Personnel ~~&~~ 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 for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and
- 1.2.4.** Cyber Security Incident response

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

- R2.** Each Responsible Entity ~~for its assets~~ with at least one asset identified in CIP-002-5, ~~Requirement R1, Part R1.3, containing low impact BES Cyber Systems~~ shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented cyber security ~~policies that collectively address~~ plan(s) for its low impact BES Cyber Systems that include the ~~following topics, and review and obtain CIP Senior~~

~~Manager approval for those policies at least once every 15 calendar months; sections in Attachment 1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]~~

~~2.1 Cyber security awareness;~~

~~2.2 Physical security controls;~~

~~2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and~~

~~2.4 Incident response to a Cyber Security Incident.~~

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.** ~~Examples of evidence may~~Evidence shall include, ~~but are not limited to, one or more each of the~~ documented cyber security ~~policies and evidence of processes, procedures, or plans~~plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate ~~the~~ implementation of the required topics; ~~revision history, records of review, or workflow evidence from a document management system that indicate review of each~~ cyber security ~~policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.~~ 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, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- M4.** An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.



## C. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority (“CEA”) unless means NERC or the applicable entity is owned, operated, or controlled byRegional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEANERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

~~Complain~~Complaints

#### 1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			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>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			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 <del>or delegate</del> within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of</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 <del>or delegate</del> within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of</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 <del>or delegate</del> 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><u>The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002</u></p>	<p>The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1)</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 <del>or delegate</del> within 18 calendar months of the</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>the previous approval. (R1.1)</p> <p><u>OR</u></p> <p><u>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 four topics required by R1. (R1.2)</u></p> <p><u>OR</u></p> <p><u>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</u></p>	<p>the previous approval. (R1.1)</p> <p><u>OR</u></p> <p><u>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 four topics required by R1. (R1.2)</u></p> <p><u>OR</u></p> <p><u>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</u></p>	<p><u>containing low impact BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2)</u></p> <p><u>OR</u></p> <p><u>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 not complete this review in less than or equal to 18 calendar months of the previous review. (R1.2)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity did not complete its approval of the one or more documented cyber</u></p>	<p>previous approval. (R1.1)</p> <p><u>OR</u></p> <p><u>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 any of the four topics required by R1. (R1.2)</u></p> <p><u>OR</u></p> <p><u>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)</u></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><u>required by Requirement R1 within 15 calendar months but did not complete this review in less than or equal to 16 calendar months of the previous review. (R1.2)</u></p> <p><u>OR</u></p> <p><u>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</u></p>	<p><u>required by Requirement R1 within 16 calendar months but did not complete this review in less than or equal to 17 calendar months of the previous review. (R1.2)</u></p> <p><u>OR</u></p> <p><u>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</u></p>	<p><u>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 17 calendar months but did not complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)</u></p>	<p><u>OR</u></p> <p><u>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 18 calendar months of the previous approval. (R1.2)</u></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>approval in less than or equal to 16 calendar months of the previous approval. (R1.2)</u>	<u>did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)</u>		
R2	Operations Planning	Lower	The Responsible Entity documented <del>and implemented one or more its</del> cyber security <del>policiesplan(s) for its</del> assets <del>with a</del> containing low impact <del>rating that address only three of the topics as required by R2 and has identified deficienciesBES Cyber Systems, but did not assess or correct the deficiencies.failed to document cyber security awareness according to CIP-003-</del>	The Responsible Entity documented <del>and implemented one or more its</del> cyber security <del>policiesplan(s) for its</del> assets <del>with a</del> containing low impact <del>rating that address only two of the topics as required by R2 and has identified deficienciesBES Cyber Systems, but did not assess or correct the deficiencies.failed to reinforce cyber security practices at least once every 15</del>	The Responsible Entity documented <del>and implemented</del> one or more <u>Cyber Security Incident response plans within its</u> cyber security <del>policiesplan(s) for its</del> assets <del>with a</del> containing low impact <del>rating that address only one of the topics as required by R2 and has identified deficienciesBES Cyber Systems, but did not assess or correct the deficiencies.failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months</del> according to CIP-003-6,	The Responsible Entity <del>did not</del> failed <u>to</u> document or implement <u>anyone or more</u> cyber security <del>policiesplan(s) for its</del> assets <del>with a</del> containing low impact <del>rating that address the topics as required by R2. (R2)</del>  OR  The Responsible Entity <del>did not</del> complete its review of the one or more documented cyber security policies for assets with a low

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><u>6, Requirement R2, Attachment 1, Section 1. (R2)</u></p> <p>OR</p> <p>The Responsible Entity documented <del>and implemented one or more its</del> cyber security <del>policies</del> <u>plan(s) for its</u> assets <del>with a</del> <u>containing</u> low impact <del>rating that address only three of the topics as required by R2</del> <u>BES Cyber Systems</u>, but <del>did not identify, assess, or correct the deficiencies.</del> <u>failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2,</u></p>	<p><u>calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2)</u></p> <p>OR</p> <p>The Responsible Entity documented <del>and implemented</del> one or more <u>incident response plans within its</u> cyber security <del>policies</del> <u>plan(s) for its</u> assets <del>with a</del> <u>containing</u> low impact <del>rating that address only two of the topics as required by BES</del> <u>Cyber Systems</u>, but <del>failed to include the process for identification, classification, and response to Cyber Security Incidents</del></p>	<p><u>Requirement R2, Attachment 1, Section 4. (R2)</u></p> <p>OR</p> <p><u>The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2)</u></p> <p>OR</p> <p><u>The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit</u></p>	<p><del>impact rating as required by R2 within 18 calendar months of the previous review. (R2)</del></p> <p>OR</p> <p><del>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the BES Cyber Systems according to CIP Senior Manager within 18 calendar months of the previous approval. CIP-003-6, Requirement R2, Attachment 1. (R2)</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><u>Attachment 1, Section 4. (R2)</u></p> <p>OR</p> <p>The Responsible Entity <del>did not complete its review of the documented</del> one or more <del>documented Cyber Security Incident response plans within its</del> cyber security <del>policies plan(s) for its</del> assets <del>with a</del>containing low impact <del>rating as required by R2</del> within 15 calendar months <del>BES Cyber Systems, but did not complete this review in less than or equal to 16 calendar months of the previous review. (R2)</del></p>	<p>according to CIP-003-6, Requirement R2 <del>but did not identify, assess, or correct the deficiencies,</del> <u>Attachment 1, Section 4. (R2)</u></p> <p><u>(R2)</u></p> <p>OR</p> <p>The Responsible Entity <del>did not complete its review of the one or more documented its</del> cyber security <del>policies plan(s) for its</del> assets <del>with a</del>containing low impact <del>rating as required by R2</del> within 16 calendar months <del>BES Cyber Systems, but did not complete this review in less than or</del></p>	<p><u>inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)</u></p> <p>OR</p> <p>The Responsible Entity documented and implemented <del>one or more cyber security policies for electronic access controls for its</del> assets <del>with a</del>containing low impact <del>rating that address only one of the topics as required by R2</del> but did not identify, assess, or correct the deficiencies.</p> <p>OR</p> <p>The Responsible Entity <del>did not complete its review of the one or more documented cyber security policies for</del> assets <del>with a</del>BES Cyber</p>	



R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>OR</del></p> <p><del>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager failed to update each Cyber Security Incident response plan(s) within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)180 days according to CIP-003-6, Requirement R2,</del></p>	<p><del>equal failed to 17 calendar months of document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the previous review. (R2)Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4.</del></p> <p>OR</p> <p>The Responsible Entity <del>did not complete its approval of the one or more documented its</del></p>	<p><del>Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)</del></p> <p>OR</p> <p>The Responsible Entity <del>did not complete its approval of the one or more documented cyber security policies the physical access controls for its assets with a containing low impact</del></p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>Attachment 1, Section 4. (R2)</u>	<p>cyber security <del>polices</del><u>plan(s)</u> for <u>its</u> assets <del>with</del> <u>a</u>containing low impact <del>rating as required by R2 by the CIP Senior Manager within 16 calendar months</del><u>BES Cyber Systems, but did complete this approval in less than or equal to 17 calendar months of the previous approval. (failed to document physical security controls according to CIP-003-6, Requirement R2), Attachment 1, Section 2. (R2)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity documented its cyber security plan(s) for its assets</u></p>	<p><del>rating as required by R2 by the CIP Senior Manager within 17 calendar months</del><u>BES Cyber Systems, but did complete this approval in less than or equal failed to 18 calendar months of the previous approval.</u> <u>implement the physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2)</u></p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p><u>containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)</u></p>		
<b>R3</b>	<b>Operations Planning</b>	<b>Medium</b>	<p>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)</p>	<p>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)</p>	<p>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)</p>	<p>The Responsible Entity has not identified, by name, a CIP Senior Manager.</p> <p>OR</p> <p>The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days of the change. (R3)
R4	Operations Planning	Lower	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	<del>The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has identified deficiencies but did not assess or correct the deficiencies.(R4)</del>  OR <del>The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4)</del>	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4)  OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>OR</del></p> <p>The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)</p>	

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

None.

Version History

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>1</u>	<u>1/16/06</u>	<u>R3.2 — Change “Control Center” to “control center.”</u>	<u>3/24/06</u>
<u>2</u>	<u>9/30/09</u>	<u>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</u> <u>Removal of reasonable business judgment.</u> <u>Replaced the RRO with the RE as a responsible entity.</u> <u>Rewording of Effective Date.</u> <u>Changed compliance monitor to Compliance Enforcement Authority.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Updated Version Number from -2 to -3</u> <u>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.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Approved by the NERC Board of Trustees.</u>	
<u>3</u>	<u>3/31/10</u>	<u>Approved by FERC.</u>	
<u>4</u>	<u>1/24/11</u>	<u>Approved by the NERC Board of Trustees.</u>	
<u>5</u>	<u>11/26/12</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</u>
<u>5</u>	<u>11/22/13</u>	<u>FERC Order issued approving CIP-003-5.</u>	
<u>6</u>	<u>11/13/14</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Addressed two FERC directives from Order No. 791 related to identify, assess, and correct</u>

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
			<u>language and communication networks.</u>
<u>6</u>	<u>2/12/2015</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>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.</u>

## CIP-003-6 - 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 Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

**Section 3.** Electronic Access Controls: Each Responsible Entity shall:

- 3.1** For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and
- 3.2** Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, 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 Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;
- 4.3** Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- 4.4** Incident handling for Cyber Security Incidents;
- 4.5** 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

**4.6** 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.

## CIP-003-6 - 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, if any, containing a LEAP.

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

- Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and 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 Sector Information Sharing and Analysis Center (ES-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.

## Guidelines and Technical Basis

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

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

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

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

#### Requirement R1:

~~The~~In developing policies in compliance with Requirement R1, the number of policies and their ~~specific language are~~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 cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1.~~ The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering ~~these~~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-~~5~~6, 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-003-6, 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 four 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-~~56~~, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-~~004003~~ through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements ~~from CIP-004 through CIP-011 in NERC cyber security Reliability Standards~~, but rather to ~~put together~~ develop a holistic cyber security policy appropriate ~~to~~ for its organization. ~~The assessment through the Compliance Monitoring and Enforcement Program Elements of a policy items that extend beyond the scope of CIP-004 through CIP-011 should~~ NERC's cyber security Reliability Standards will not be considered candidates for potential violations. ~~The Responsible Entity should consider the following for each although they will help demonstrate the organization's internal culture of the required topics in its compliance and posture towards cyber security policy:~~

For Part 1.1, the Responsible Entity should 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

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

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

As with Requirement R1, Using the numberlist of policies-assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a general information security program for the entire organization or as components of specific program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

### **Requirement R2, Attachment 1**

As noted, Attachment 1 contains the sections that must be 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. The cyber security policy must cover in sufficient detail used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four topicalsubject matter areas required by CIP-003-5, 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 Responsible Entityentity has flexibility to develop a single comprehensive cyber security policy coveringthe discretion to determine the topics to be addressed and the manner in which it will communicate these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy. As evidence of compliance, the Responsible Entity would be expected to provide the high-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 Responsible Entity is not 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) low impact BES Cyber Systems at assets containing low impact BES Cyber System(s) and (2) LEAPs, if any. If the LEAP is located within the BES asset and inherits the same controls outlined in Section 2, this can 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 in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems, the low impact BES Cyber Systems themselves, or LEAPs, if any. The Responsible Entity may use one or a combination of 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. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level ~~policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this~~ for access to the site or systems, including LEAPs. ~~The requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (does not obligate an entity to specify a need for each access or authorization of a user for access.~~

Monitoring as a physical security control can be used ~~as of this writing) of reviewing a~~ complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into ~~a statistical sample of systems is not necessary. The SDT also notes that in topic 2.3, the SDT uses the~~ 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 monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

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

Section 3 requires the establishment of boundary protections for low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable



protocols or Dial-up Connectivity. The term “electronic access control” is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude “point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems,” such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases “direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.” The intent of “direct” in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for “device-to-device connection,” LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple

assets containing low impact BES Cyber Systems “behind” it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a “pass-through” of the data flow communication, then that “pass-through” data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

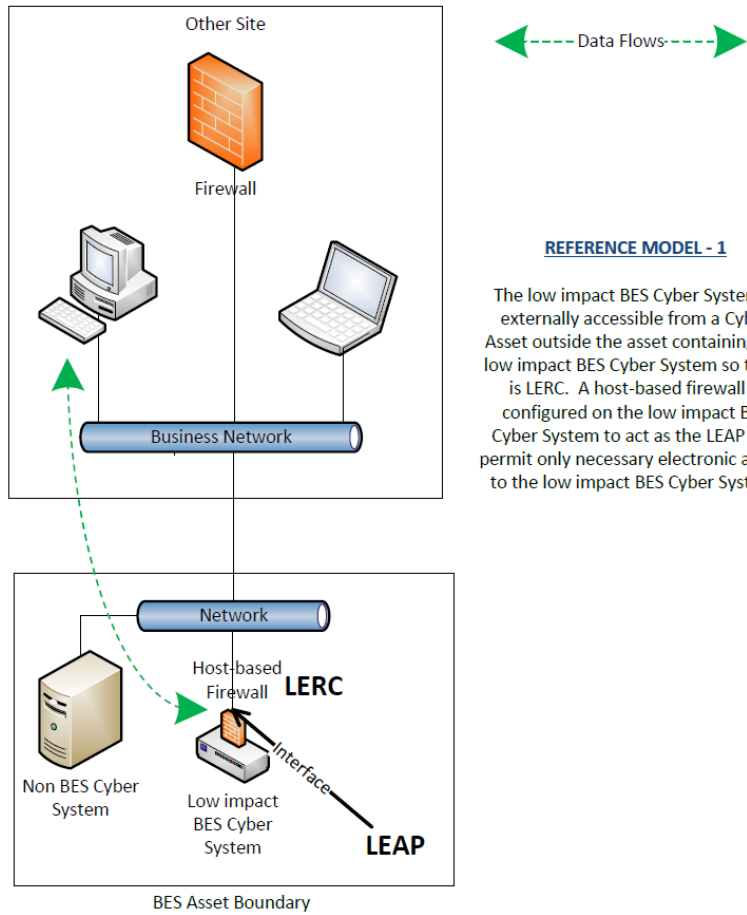
- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a “protocol break” so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.

- 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.

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

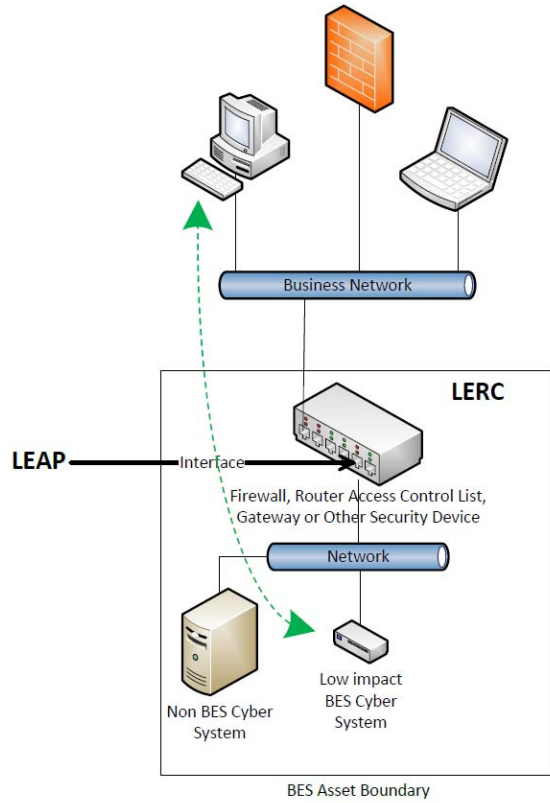
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a 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.
- In Reference Model 5, using just 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 and the business network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.



**REFERENCE MODEL - 1**

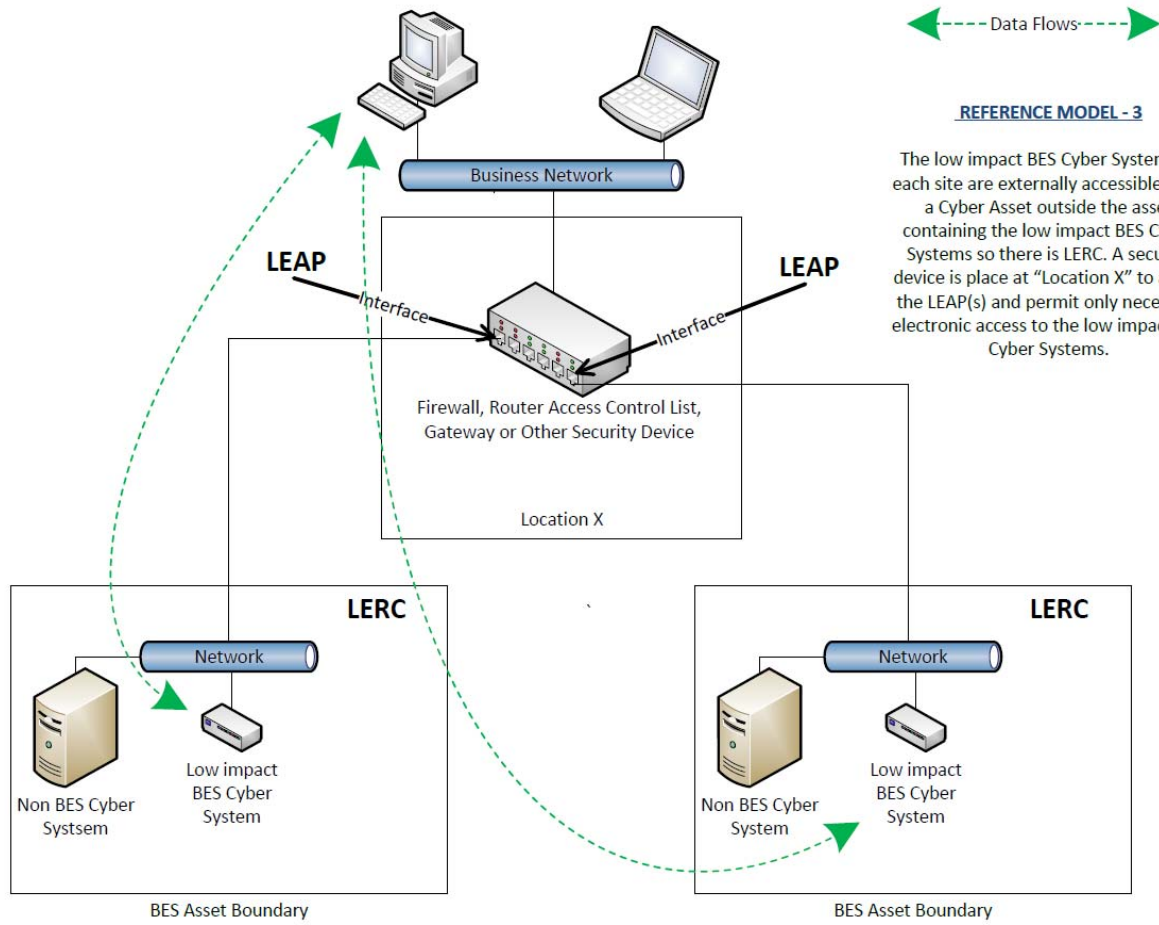
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.



← Data Flows →

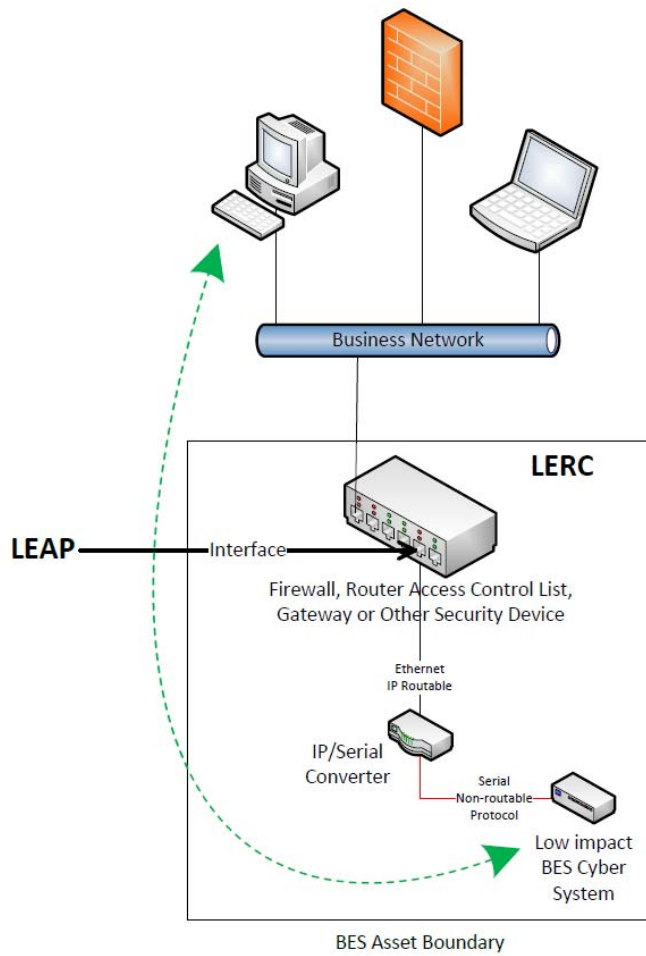
**REFERENCE MODEL - 2**

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.



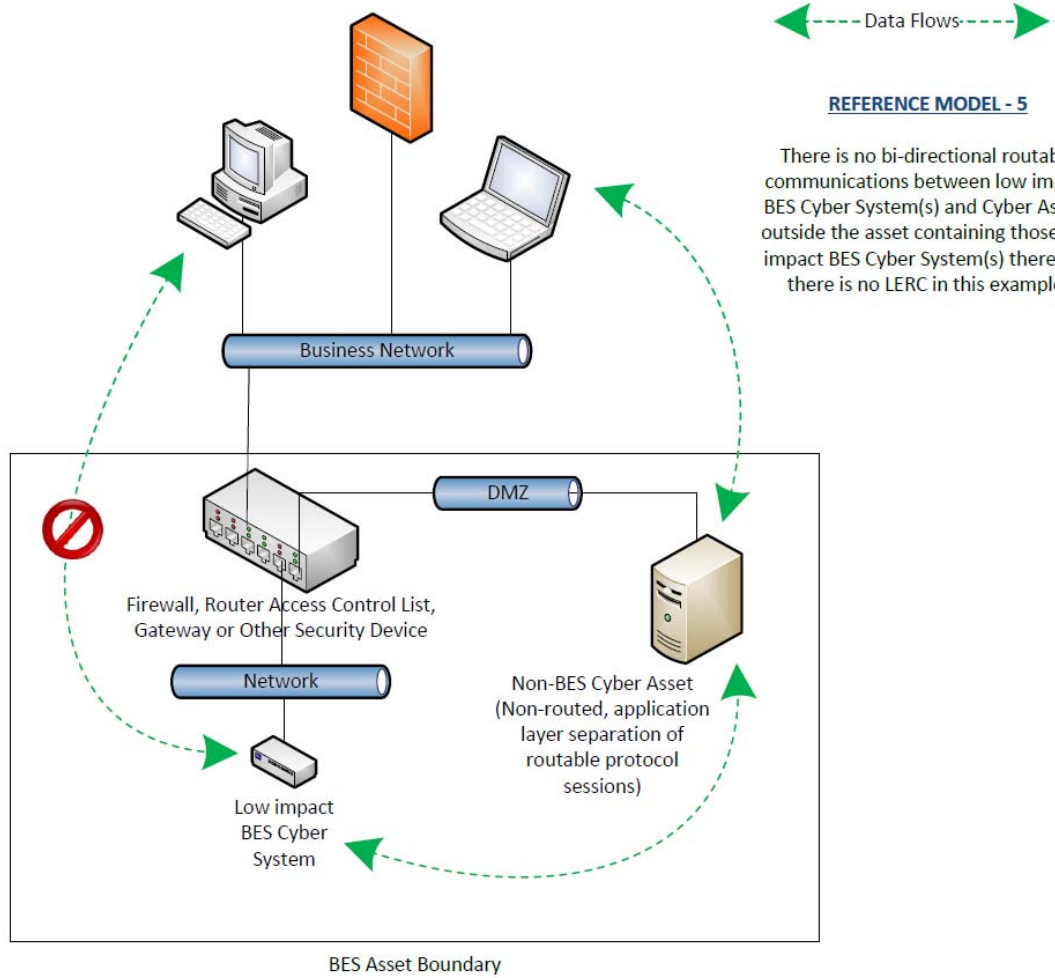
**REFERENCE MODEL - 3**

The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is placed at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.

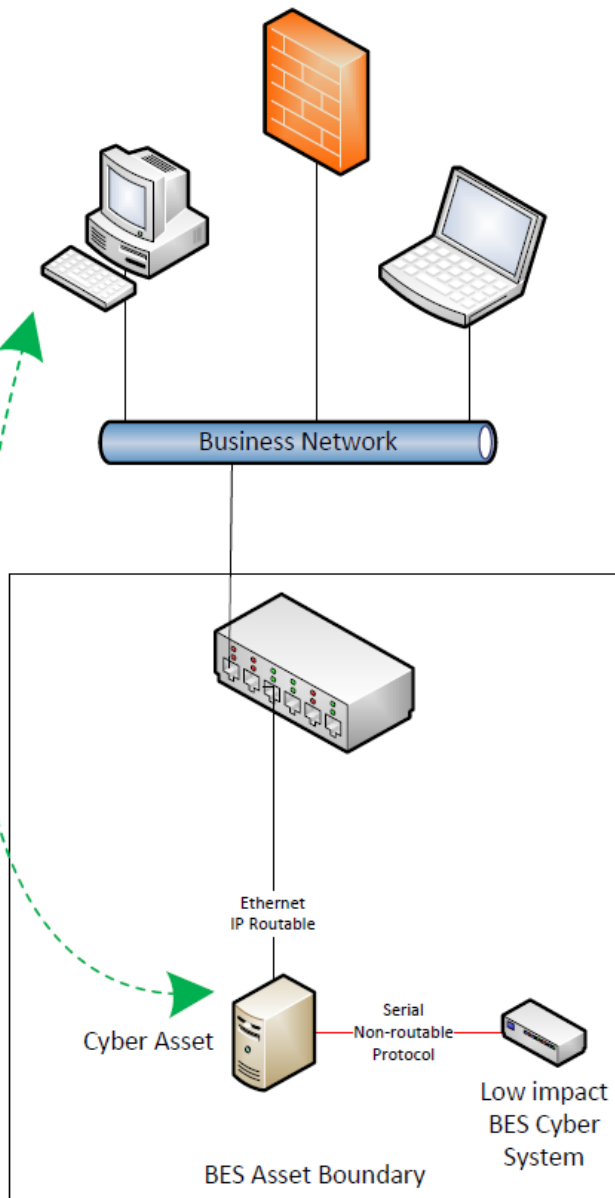


**REFERENCE MODEL - 4**

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

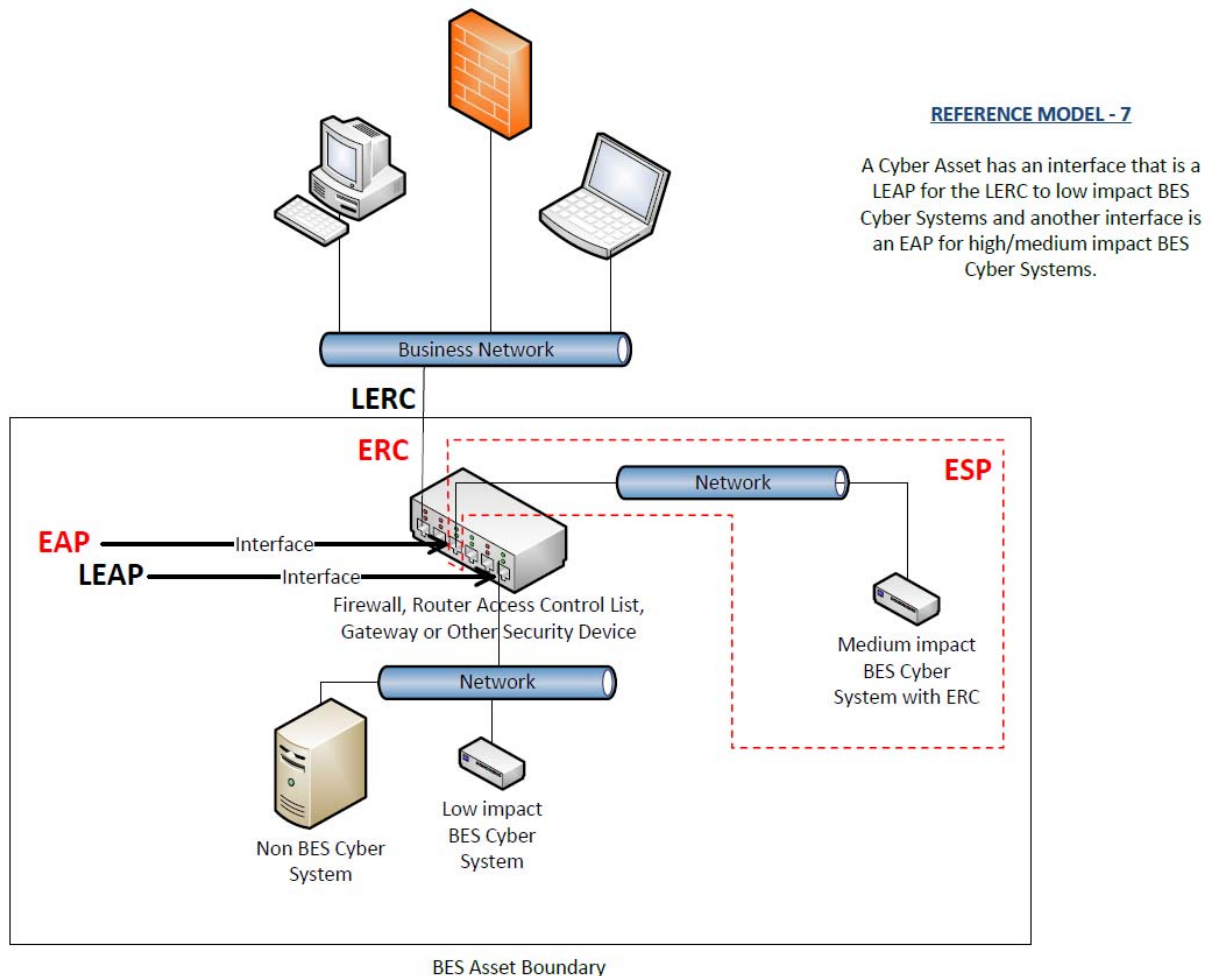






**REFERENCE MODEL - 6**

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



**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 Systems, 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 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 R3:**

The intent of CIP-003-~~56~~, 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 ~~this~~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-~~56~~, 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 ~~should have~~ significant flexibility to adapt this requirement to theirs existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records ~~provides~~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 the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

## Rationale:

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

### Rationale for Requirement R1:

One or more security policies enable effective implementation of the ~~standard's 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 ~~personnel who have authorized electronic access and/or authorized unescorted physical access to its~~ 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 ~~standard's requirements.~~

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

### Rationale for Requirement R2:

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

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

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

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 Systems. The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. 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 Systems. However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

#### **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.

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

### Version History

Version	Date	Action	Change Tracking
1	1/16/06	<del>R3.2 — Change “Control Center” to “control center.”</del>	3/24/06
2	9/30/09	<del>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.</del>	
3	12/16/09	<del>Updated version number from 2 to 3. Approved by the NERC Board of Trustees.</del>	
3	3/31/10	Approved by FERC.	

Guidelines and Technical Basis

---

4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5. (Order becomes effective 2/3/14.)	
5	4/2/14	Address directive in FERC Order 791 to modify VSLs for Requirements R1 and R2	R1 and R2 — VSLs

**Reliability Standard CIP-004-6 Clean and Redline**



## A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-6
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

### 4. Applicability:

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

#### 4.1.1. Balancing Authority

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

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

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

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

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

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

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

#### 4.1.3. Generator Operator

#### 4.1.4. Generator Owner

#### 4.1.5. Interchange Coordinator or Interchange Authority

**4.1.6. Reliability Coordinator**

**4.1.7. Transmission Operator**

**4.1.8. Transmission Owner**

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

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

**4.2.1.1.** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3. Exemptions:** The following are exempt from Standard CIP-004-6:

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

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

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

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

**4.2.3.5.** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. Effective Dates:**

See Implementation Plan for CIP-004-6.

**6. Background:**

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

**“Applicable Systems” Columns in Tables:**

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

**B. Requirements and Measures**

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	<p>An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as:</p> <ul style="list-style-type: none"> <li>• direct communications (for example, e-mails, memos, computer-based training); or</li> <li>• indirect communications (for example, posters, intranet, or brochures); or</li> <li>• management support and reinforcement (for example, presentations or meetings).</li> </ul>

- R2.** Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]
- M2.** Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Training content on:</p> <ol style="list-style-type: none"> <li>2.1.1. Cyber security policies;</li> <li>2.1.2. Physical access controls;</li> <li>2.1.3. Electronic access controls;</li> <li>2.1.4. The visitor control program;</li> <li>2.1.5. Handling of BES Cyber System Information and its storage;</li> <li>2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan;</li> <li>2.1.7. Recovery plans for BES Cyber Systems;</li> <li>2.1.8. Response to Cyber Security Incidents; and</li> <li>2.1.9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.</li> </ol>	<p>Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.</p>

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.</p>	<p>Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Require completion of the training specified in Part 2.1 at least once every 15 calendar months.</p>	<p>Examples of evidence may include, but are not limited to, dated individual training records.</p>



- R3.** Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M3.** Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> <li>3.2.1. current residence, regardless of duration; and</li> <li>3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.</li> </ol> <p>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to perform a seven year criminal history records check.</p>

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Criteria or process to evaluate criminal history records checks for authorizing access.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to evaluate criminal history records checks.</p>
3.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments.</p>

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.</p>

- R4.** Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program*. [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning and Same Day Operations*].
- M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ol style="list-style-type: none"> <li>4.1.1. Electronic access;</li> <li>4.1.2. Unescorted physical access into a Physical Security Perimeter; and</li> <li>4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.</li> </ol>	<p>An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.</p>

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or</li> <li>• Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).</li> </ul>

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.</p>	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> <li>1. A dated listing of all accounts/account groups or roles within the system;</li> <li>2. A summary description of privileges associated with each group or role;</li> <li>3. Accounts assigned to the group or role; and</li> <li>4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.</li> </ol>

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.</p>	<p>An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> <li>1. A dated listing of authorizations for BES Cyber System information;</li> <li>2. Any privileges associated with the authorizations; and</li> <li>3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.</li> </ol>



- R5.** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated workflow or sign-off form verifying access removal associated with the termination action; and</li> <li>2. Logs or other demonstration showing such persons no longer have access.</li> </ol>

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated workflow or sign-off form showing a review of logical and physical access; and</li> <li>2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.</li> </ol>

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.</p>	<p>An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.</p>

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> <li>EACMS</li> </ul>	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.5	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> <li>EACMS</li> </ul>	<p>For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p> <p>If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>Workflow or sign-off form showing password reset within 30 calendar days of the termination;</li> <li>Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or</li> <li>Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.</li> </ul>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Additional Compliance Information:

None

**2. Table of Compliance Elements**

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R1</b>	<b>Operations Planning</b>	<b>Lower</b>	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1)  OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
<b>R2</b>	<b>Operations Planning</b>	<b>Lower</b>	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1)  OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1)  OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)  OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p>	<p>The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)</p>	<p>The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)</p>	<p>The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p> <p>OR</p>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)</p>			<p>The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)</p>
<b>R3</b>	<b>Operations Planning</b>	<b>Medium</b>	<p>The Responsible Entity has a program for conducting</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including</p>	<p>The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,</p>	<p>contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,</p>	<p>contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,</p>	<p>within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3)</p> <p>OR</p> <p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3)</p> <p>OR</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized</p>	<p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)</p>	<p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)</p>	<p>or more individuals. (3.2 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
<b>R4</b>	<b>Operations Planning and Same Day Operations</b>	<b>Medium</b>	<p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)</p>	<p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct</p>	<p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct</p>	<p>The Responsible Entity did not implement any documented program(s) for access management. (R4)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or</p>	<p>and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were</p>	<p>and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were</p>	<p>OR</p> <p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)



R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			locations, privileges were incorrect or unnecessary. (4.4)			
<b>R5</b>	<b>Same Day Operations and Operations Planning</b>	<b>Medium</b>	<p>The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time</p>	<p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of</p>	<p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of</p>	<p>The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>of the termination action. (5.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4)</p> <p>OR</p>	<p>access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the</p>	<p>access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective</p>	<p>removals for three or more individuals. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR	termination action. (5.3)	date and time of the termination action. (5.3)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating</p>			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.5)			

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

None.

**Version History**

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

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/2015	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.

## Guidelines and Technical Basis

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

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

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

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

#### Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

#### Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but



a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

### **Requirement R3:**

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

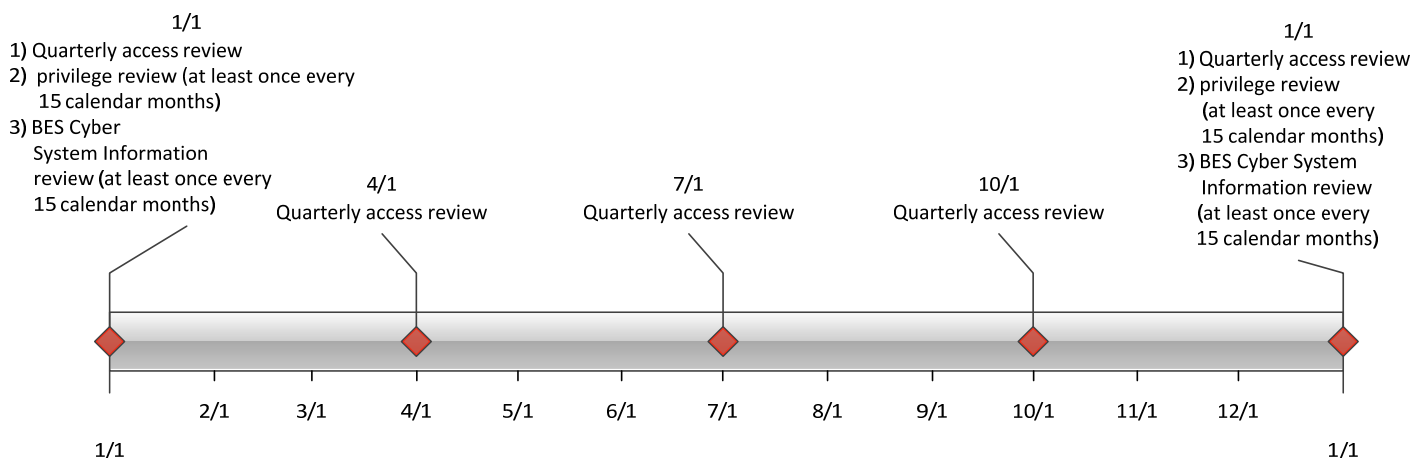
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

**Requirement R4:**

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual’s associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

**Requirement R5:**

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

### **Rationale:**

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

### **Rationale for Requirement R1:**

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such

authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

**Rationale for Requirement R2:**

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

**Rationale for Requirement R3:**

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

**Rationale for Requirement R4:**

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

### **Rationale for Requirement R5:**

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

## A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-~~5-16~~
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

### 4. Applicability:

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

#### 4.1.1. Balancing Authority

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

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

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

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

**4.1.2.2.** Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

**4.2.1.1.** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3. Exemptions:** The following are exempt from Standard CIP-004-~~5.16~~:

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

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

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



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

**4.2.3.5.** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~5.1~~ identification and categorization processes.

**5. ~~5.~~ Effective Dates:**

~~1. **24 Months Minimum**—CIP 004 5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP 004 5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-004-6.

**6. Background:**

Standard CIP-004-~~5.1~~ exists as part of a suite of CIP Standards related to cyber security. ~~CIP-002-5 requires, which require~~ the initial identification and categorization of BES Cyber Systems. ~~CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 and~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.~~

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 of the requirements.

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

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

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

~~not required to include the “. . . identifies, assesses, and corrects deficiencies, . . .” elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

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

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

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

Measures 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~~. 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 CS0706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

**B. Requirements and Measures**

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.16 Table R1 – Security Awareness Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.16 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5.16 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: <ul style="list-style-type: none"> <li>• direct communications (for example, e-mails, memos, computer-based training); or</li> <li>• indirect communications (for example, posters, intranet, or brochures); or</li> <li>• management support and reinforcement (for example, presentations or meetings).</li> </ul>

- R2.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies, a one or more~~ cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~5.16~~ Table R2 – Cyber Security Training Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M2.** Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~5.16~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5.16 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Training content on:</p> <ol style="list-style-type: none"> <li>2.1.1. Cyber security policies;</li> <li>2.1.2. Physical access controls;</li> <li>2.1.3. Electronic access controls;</li> <li>2.1.4. The visitor control program;</li> <li>2.1.5. Handling of BES Cyber System Information and its storage;</li> <li>2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan;</li> <li>2.1.7. Recovery plans for BES Cyber Systems;</li> <li>2.1.8. Response to Cyber Security Incidents; and</li> <li>2.1.9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, <u>including Transient Cyber Assets, and with Removable Media.</u></li> </ol>	<p>Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.</p>

CIP-004-5.16 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.</p>	<p>Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Require completion of the training specified in Part 2.1 at least once every 15 calendar months.</p>	<p>Examples of evidence may include, but are not limited to, dated individual training records.</p>

- R3.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment ~~programs~~program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~5.16~~ Table R3 – Personnel Risk Assessment Program*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M3.** Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.16~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004- <del>5.16</del> Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to confirm identity.



CIP-004-5.16 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> <li>3.2.1. current residence, regardless of duration; and</li> <li>3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.</li> </ol> <p>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to perform a seven year criminal history records check.</p>

CIP-004-5.16 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Criteria or process to evaluate criminal history records checks for authorizing access.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to evaluate criminal history records checks.</p>
3.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments.</p>

CIP-004-5.16 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.</p>

- R4.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management ~~programs~~program(s) that collectively include each of the applicable requirement parts in CIP-004-~~5.16~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in CIP-004-~~5.16~~ Table R4 – Access Management Program and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004- <del>5.16</del> Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ol style="list-style-type: none"> <li>4.1.1. Electronic access;</li> <li>4.1.2. Unescorted physical access into a Physical Security Perimeter; and</li> <li>4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.</li> </ol>	<p>An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.</p>

CIP-004-5.16 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or</li> <li>• Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).</li> </ul>

CIP-004-5.16 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.</p>	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> <li>1. A dated listing of all accounts/account groups or roles within the system;</li> <li>2. A summary description of privileges associated with each group or role;</li> <li>3. Accounts assigned to the group or role; and</li> <li>4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.</li> </ol>

CIP-004-5.16 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.</p>	<p>An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> <li>1. A dated listing of authorizations for BES Cyber System information;</li> <li>2. Any privileges associated with the authorizations; and</li> <li>3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.</li> </ol>

- R5.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation ~~programs~~ program(s) that collectively include each of the applicable requirement parts in CIP-004-~~5.16~~ Table R5 – Access Revocation. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in CIP-004-~~5.16~~ Table R5 – Access Revocation and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- <del>5.16</del> Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated workflow or sign-off form verifying access removal associated with the termination action; and</li> <li>2. Logs or other demonstration showing such persons no longer have access.</li> </ol>



CIP-004-5.16 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated workflow or sign-off form showing a review of logical and physical access; and</li> <li>2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.</li> </ol>

CIP-004-5.16 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.</p>	<p>An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.</p>

CIP-004-5.16 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> <li>EACMS</li> </ul>	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-5.16 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.5	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> <li>EACMS</li> </ul>	<p>For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p> <p>If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>Workflow or sign-off form showing password reset within 30 calendar days of the termination;</li> <li>Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or</li> <li>Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.</li> </ul>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority (“(“ (CEA”) unless) means NERC or the applicable entity is owned, operated, or controlled by Regional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEANERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Violation Investigations

Self-Reporting

- ~~Complaint~~

Complaints

#### 1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1)  OR  The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)  OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>content topics in Requirement Parts 2.1.1 through 2.1.9; <del>and did not identify, assess and correct the deficiencies.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized</p>	<p><del>and correct the deficiencies.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access; <del>and did not identify, assess and correct the deficiencies.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized</p>	<p><del>and correct the deficiencies.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access; <del>and did not identify, assess and correct the deficiencies.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized</p>	<p>The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9; <del>and did not identify, assess and correct the deficiencies.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access; <del>and did not</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>unescorted physical access, <del>and did not identify, assess and correct the deficiencies.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion</p>	<p>electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, <del>and did not identify, assess and correct the deficiencies.</del> (2.3), (2.3)</p>	<p>unescorted physical access within 15 calendar months of the previous training completion date, <del>and did not identify, assess and correct the deficiencies.</del> (2.3), (2.3)</p>	<p><del>identify, assess and correct the deficiencies.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, <del>and did not identify, assess and correct the deficiencies.</del> (2.3), (2.3)</p>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<del>date, and did not identify, assess and correct the deficiencies. (2.3), (2.3)</del>			
<b>R3</b>	<b>Operations Planning</b>	<b>Medium</b>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including</p>	<p>The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3)</p> <p>OR</p> <p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>for one individual, <del>and did not identify, assess, and correct the deficiencies.</del> (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one</p>	<p>contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (3.1 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, <del>and did not identify, assess, and</del></p>	<p>contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (3.1 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, <del>and did not identify, assess, and</del></p>	<p>for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (3.1 &amp; 3.4)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- <del>5-16</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>individual, and did not identify, assess, and correct the deficiencies.</del> (3.1 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required</p>	<p><del>correct the deficiencies.</del> (3.2 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (3.3 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted</p>	<p><del>correct the deficiencies.</del> (3.2 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (3.3 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted</p>	<p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (3.2 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>checks described in 3.2.1 and 3.2.2 for one individual, <del>and did not identify, assess, and correct the deficiencies.</del> (3.2 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access</p>	<p>physical access within 7 calendar years of the previous PRA completion date, <del>and did not identify, assess, and correct the deficiencies.</del> (3.5). (3.5)</p>	<p>physical access within 7 calendar years of the previous PRA completion date, <del>and did not identify, assess, and correct the deficiencies.</del> (3.5). (3.5)</p>	<p>authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (3.3 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date <del>and has identified deficiencies, and did not identify, assess, and correct the deficiencies.</del> (3.5). (3.5)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>but did not evaluate criminal history records check for access authorization for one individual, <del>and did not identify, assess, and correct the deficiencies.</del> (3.3 &amp; 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7</p>			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- <del>5.16</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, <del>and did not identify, assess, and correct the deficiencies.</del> (3.5). (3.5)			
R4	Operations Planning and Same Day Operations	Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter, <del>and did not identify, assess, and correct the deficiencies.</del> (4.2)  OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter, <del>and did not identify, assess, and correct the deficiencies.</del> (4.2)  OR	The Responsible Entity did not implement any documented program(s) for access management. (R4)  OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- <del>5.16</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>of a subsequent calendar quarter, <del>and did not identify, assess and correct the deficiencies.</del> (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15</p>	<p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary, <del>and did not identify, assess, and correct the deficiencies.</del> (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System</p>	<p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, <del>and did not identify, assess, and correct the deficiencies.</del> (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System</p>	<p>BES Cyber System Information is located, <del>and did not identify, assess, and correct the deficiencies.</del> (4.1). (4.1)</p> <p>OR</p> <p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, <del>and did not identify, assess, and correct the deficiencies.</del> (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary, <del>and did not identify, assess and correct the deficiencies.</del> (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, <del>and did not identify, assess, and correct the deficiencies.</del> <del>(4.4).</del> (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, <del>and did not identify, assess, and correct the deficiencies.</del> <del>(4.4).</del> (4.4)	role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, <del>and did not identify, assess, and correct the deficiencies.</del> (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System



R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary; <del>and did not identify, assess and correct the deficiencies. (4.4) - (4.4)</del>			Information storage locations, privileges were incorrect or unnecessary; <del>and did not identify, assess, and correct the deficiencies. (4.4) - (4.4)</del>
R5	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more process(es) to	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			revoke the individual’s access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, <del>and did not identify, assess, and correct the deficiencies.</del> (5.3) OR The Responsible	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, <del>and did not identify, assess, and correct the deficiencies.</del> (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted	physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (5.1) OR The Responsible Entity has implemented one or more process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- <del>5.16</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to revoke the individual’s user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (5.4) OR The Responsible Entity has implemented	physical access by the end of the next calendar day following the predetermined date, <del>and did not identify, assess, and correct the deficiencies.</del> (5.2). (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, <del>and did not identify, assess, and correct the deficiencies.</del> (5.3). (5.3)	physical access by the end of the next calendar day following the predetermined date, <del>and did not identify, assess, and correct the deficiencies.</del> (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, <del>and did not identify, assess, and correct the deficiencies.</del> (5.3). (5.3)	determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, <del>and did not identify, assess, and correct the deficiencies.</del> (5.2). (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, <del>and did not identify, assess, and correct the deficiencies.</del> (5.5) OR			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.16)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating</p>			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- <del>5.16</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances, <del>and did not</del> <del>identify, assess,</del> <del>and correct the</del> <del>deficiencies.</del> <del>(5.5).</del> (5.5)			

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

None.

**Version History**

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>1</u>	<u>1/16/06</u>	<u>R3.2 — Change “Control Center” to “control center.”</u>	<u>3/24/06</u>
<u>2</u>	<u>9/30/09</u>	<u>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</u> <u>Removal of reasonable business judgment.</u> <u>Replaced the RRO with the RE as a responsible entity.</u> <u>Rewording of Effective Date.</u> <u>Changed compliance monitor to Compliance Enforcement Authority.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Updated Version Number from -2 to -3</u> <u>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.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Approved by the NERC Board of Trustees.</u>	
<u>3</u>	<u>3/31/10</u>	<u>Approved by FERC.</u>	
<u>4</u>	<u>1/24/11</u>	<u>Approved by the NERC Board of Trustees.</u>	

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>5</u>	<u>11/26/12</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</u>
<u>5</u>	<u>11/22/13</u>	<u>FERC Order issued approving CIP-004-5.</u>	
<u>5.1</u>	<u>9/30/13</u>	<u>Modified two VSLs in R4</u>	<u>Errata</u>
<u>6</u>	<u>11/13/14</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.</u>
<u>6</u>	<u>2/12/2015</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>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.</u>



## 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~~5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

#### Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

#### Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

### **Requirement R3:**

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

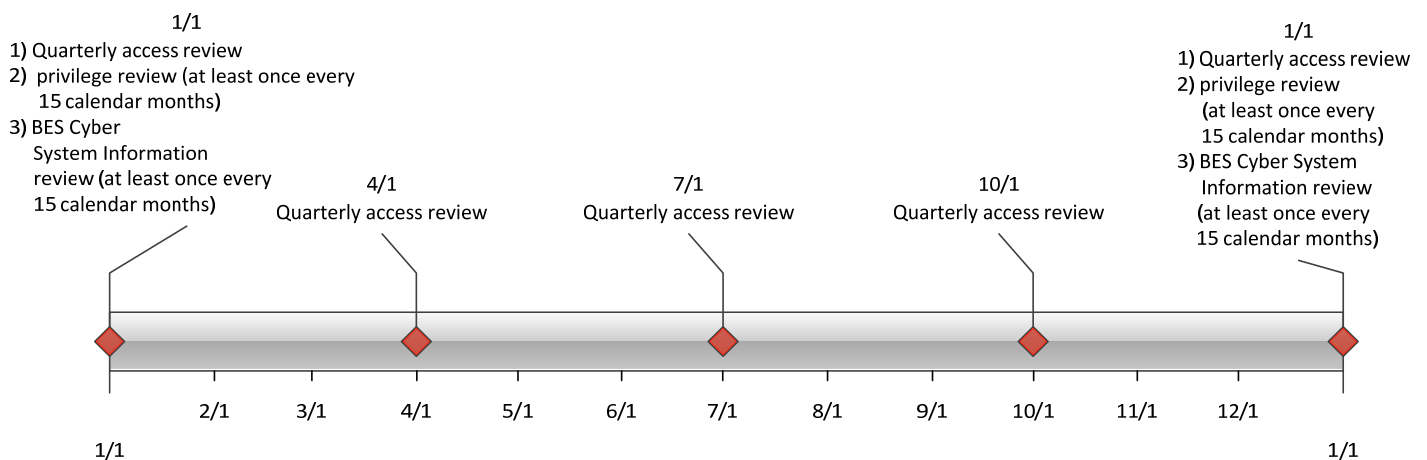
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

**Requirement R4:**

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual’s associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

**Requirement R5:**

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

### Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts text boxes~~ were embedded within the standard ~~-~~ to explain the rationale for various parts of the standard. Upon BOT approval, ~~that information~~ the text from the rationale text boxes was moved to this section.

### Rationale for **Requirement R1**:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such

authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

~~**Summary of Changes:** Reformatted into table structure.~~

~~**Reference to prior version:** (Part 1.1) CIP-004-4, R1~~

~~**Change Rationale:** (Part 1.1)~~

~~Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical access "received" ongoing reinforcement—to state that security awareness has been reinforced.~~

~~Moved example mechanisms to guidance.~~

### **Rationale for Requirement R2:**

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

~~Based on their role, some personnel may not require training on all topics.~~

### ~~**Summary of Changes:**~~

#### ~~1. Addition of specific role training for:~~

- ~~• The visitor control program~~
- ~~• Electronic interconnectivity supporting the operation and control of BES Cyber Systems~~
- ~~• Storage media as part of the handling of BES Cyber Systems information~~

#### ~~2. Change references from Critical Cyber Assets to BES Cyber Systems.~~

~~**Reference to prior version:** (Part 2.1) CIP004-4, R2.2.1~~

~~**Change Rationale:** (Part 2.1)~~

~~Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core~~

~~training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.~~

~~Reference to prior version: (Part 2.2) CIP004-4, R2.1~~

~~Change Rationale: (Part 2.2)~~

~~Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.~~

~~Reference to prior version: (Part 2.3) CIP004-4, R2.3~~

~~Change Rationale: (Part 2.3)~~

~~Updated to replace “annually” with “once every 15 calendar months.”~~

### Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

~~Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.~~

~~Reference to prior version: (Part 3.1) CIP004-4, R3.1~~

~~Change Rationale: (Part 3.1)~~

~~Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.~~

~~Reference to prior version: (Part 3.2) CIP004-4, R3.1~~

~~Change Rationale: (Part 3.2)~~

~~Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.~~

~~Reference to prior version: (Part 3.3) New~~

~~Change Rationale: (Part 3.3)~~

~~There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.~~

~~Reference to prior version: (Part 3.4) CIP-004-4, R3.3~~

~~Change Rationale: (Part 3.4)~~

~~Separated into its own table item.~~

~~Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3~~

~~Change Rationale: (Part 3.5)~~

~~Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3~~

**Rationale for Requirement R4:**

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-56. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-56 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.



For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

**Summary of Changes:** ~~The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.~~

**Reference to prior version:** ~~(Part 4.1) CIP-003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1~~

**Change Rationale:** ~~(Part 4.1)~~

~~Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a “need to know” basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.~~

**Reference to prior version:** ~~(Part 4.2) CIP-004-4, R4.1~~

**Change Rationale:** ~~(Part 4.2)~~

~~Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term “review” entailed in CIP-004-4,~~

**Requirement R4.1.** ~~This requirement clarifies the review should occur between the provisioned access and authorized access.~~

**Reference to prior version:** (Part 4.3) CIP-007-4, R5.1.3

**Change Rationale:** (Part 4.3)

*Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.*

**Reference to prior version:** (Part 4.4) CIP-003-4, R5.1.2

**Change Rationale:** (Part 4.4)

*Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*

**Rationale for Requirement R5:**

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

~~**Summary of Changes:** FERC Order No. 706, Paragraphs 460 and 461, state the following: “The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).~~

~~As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.”~~

~~**Reference to prior version:** (Part 5.1) CIP-004-4, R4.2~~

~~**Change Rationale:** (Part 5.1)~~

~~The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards to **require immediate revocation** for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.~~

~~**Reference to prior version:** (Part 5.2) CIP-004-4, R4.2~~

~~**Change Rationale:** (Part 5.2)~~

~~FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in~~

~~accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.~~

~~Reference to prior version: (Part 5.3) New~~

~~Change Rationale: (Part 5.3)~~

~~FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.~~

~~Reference to prior version: (Part 5.4) New~~

~~Change Rationale: (Part 5.4)~~

~~FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.~~

~~Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3~~

~~Change Rationale: (Part 5.5)~~

~~To provide clarification of expected actions in managing the passwords.~~

## 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.
5.1	9/30/13	Modified two VSLs in R4.	Errata
5.1	11/22/13	FERC Order issued approving CIP-004-5.1. (Order becomes effective on 2/3/14.)	
5.1	4/2/14	Address FERC Order 791 directive to modify Requirement R4 VRF and VSLs	R4 – VRF and VSLs

**Reliability Standard CIP-006-6 Clean and Redline**

## A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems
2. **Number:** CIP-006-6
3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan 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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

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

#### 4.1.3 **Generator Operator**

#### 4.1.4 **Generator Owner**

#### 4.1.5 **Interchange Coordinator or Interchange Authority**

#### 4.1.6 **Reliability Coordinator**

**4.1.7 Transmission Operator**

**4.1.8 Transmission Owner**

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

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-006-6:

**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-002-5.1 identification and categorization processes.

**5. Effective Dates:**

See Implementation Plan for CIP-006-6.

**6. Background:**

Standard CIP-006 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 “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable 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.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **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.
- **Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.



**B. Requirements and Measures**

- R1.** Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].
- M1.** Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity  Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.2	<p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.</p>

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.</p>	<p>An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.</p>

CIP-006-6 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.</p>
1.6	<p>Physical Access Control Systems (PACS) associated with:</p> <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	<p>Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.</p>	<p>An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.</p>



CIP-006-6 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.7	<p>Physical Access Control Systems (PACS) associated with:</p> <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	<p>Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.</p>

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.8	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.</p>

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.9	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.</p>	<p>An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.</p>

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.10	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> <li>• PCA</li> </ul> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ul style="list-style-type: none"> <li>• PCA</li> </ul>	<p>Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.</p> <p>Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:</p> <ul style="list-style-type: none"> <li>• encryption of data that transits such cabling and components; or</li> <li>• monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or</li> <li>• an equally effective logical protection.</li> </ul>	<p>An example of evidence may include, but is not limited to, records of the Responsible Entity’s implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.</p>

- R2.** Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]
- M2.** Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.</p>	<p>An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.</p>

CIP-006-6 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.</p>	<p>An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Retain visitor logs for at least ninety calendar days.</p>	<p>An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.</p>

- R3.** Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
- M3.** Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	Applicable Systems	Requirement	Measures
3.1	<p>Physical Access Control Systems (PACS) associated with:</p> <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul> <p>Locally mounted hardware or devices at the Physical Security Perimeter associated with:</p> <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	<p>Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.</p>	<p>An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.</p>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

#### 1.4. Additional Compliance Information:

None



**2. Table of Compliance Elements**

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning Same-Day Operations	Medium	N/A	N/A	N/A	<p>The Responsible Entity did not document or implement physical security plans. (R1)</p> <p>OR</p> <p>The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented physical</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3)</p> <p>OR</p> <p>The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4)</p> <p>OR</p> <p>The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel.</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
<b>R2</b>	<b>Same-Day Operations</b>	<b>Medium</b>	N/A	N/A	N/A	<p>The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1)</p> <p>OR</p> <p>The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor’s name, and the point of</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
<b>R3</b>	<b>Long Term Planning</b>	<b>Medium</b>	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

**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	



Version	Date	Action	Change Tracking
		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.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.

## 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.

#### **General:**

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed “six-wall” boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

#### **Requirement R1:**

Methods of physical access control include:

- **Card Key:** A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- **Special Locks:** These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- **Security Personnel:** Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

### **Requirement R2:**

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

### **Requirement R3:**

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

### **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:**

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable

communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

**Rationale for Requirement R2:**

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

**Rationale for Requirement R3:**

To ensure all Physical Access Control Systems and devices continue to function properly.

## A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems
2. **Number:** CIP-006-56
3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan 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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

**4.2.1.2** Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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-006-56:

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

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

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



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

**4.2.3.5** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. Effective Dates:**

~~1. **24 Months Minimum**— CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~See Implementation Plan for CIP-006-6.~~

**6. Background:**

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

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

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

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

processes, but they must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the "... identifies, assesses, and corrects deficiencies, ..." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

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

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

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

Measures 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-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable 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.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **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.
- **Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

**B. Requirements and Measures**

- R1.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented physical security ~~plans~~plan(s) that collectively include all of the applicable requirement parts in ~~CIP-006-56~~ *Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*.
- M1.** Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in ~~CIP-006-56~~ *Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-56 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity  Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-56 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.2	<p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.</p>

CIP-006-56 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-56 Table R1— Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.</p>	<p>An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.</p>

CIP-006-56 Table R1— Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.</p>
1.6	<p>Physical Access Control Systems (PACS) associated with:</p> <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	<p>Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.</p>	<p>An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.</p>



CIP-006-56 Table R1— Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.7	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-56 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.8	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.</p>

CIP-006-56 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.9	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.</p>	<p>An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.</p>

<u>CIP-006-6 Table R1 — Physical Security Plan</u>			
<u>Part</u>	<u>Applicable Systems</u>	<u>Requirements</u>	<u>Measures</u>
<u>1.10</u>	<p><u>High Impact BES Cyber Systems and their associated:</u></p> <ul style="list-style-type: none"> <li>• <u>PCA</u></li> </ul> <p><u>Medium Impact BES Cyber Systems at Control Centers and their associated:</u></p> <ul style="list-style-type: none"> <li>• <u>PCA</u></li> </ul>	<p><u>Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.</u></p> <p><u>Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:</u></p> <ul style="list-style-type: none"> <li>• <u>encryption of data that transits such cabling and components; or</u></li> <li>• <u>monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or</u></li> <li>• <u>an equally effective logical protection.</u></li> </ul>	<p><u>An example of evidence may include, but is not limited to, records of the Responsible Entity’s implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.</u></p>

- R2.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented visitor control ~~programs~~program(s) that include each of the applicable requirement parts in CIP-006-56 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]
- M2.** Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in CIP-006-56 Table R2 – Visitor Control Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-56 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.</p>	<p>An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.</p>

CIP-006-56 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.</p>	<p>An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Retain visitor logs for at least ninety calendar days.</p>	<p>An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.</p>

- R3.** Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-006-56 Table R3 – Maintenance and Testing Program*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
- M3.** Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-56 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-56 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	Applicable Systems	Requirement	Measures
3.1	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul> Locally mounted hardware or devices at the Physical Security Perimeter associated with: <ul style="list-style-type: none"> <li>• High Impact BES Cyber Systems, or</li> <li>• Medium Impact BES Cyber Systems with External Routable Connectivity</li> </ul>	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority (“CEA”) unless means NERC or the applicable entity is owned, operated, or controlled by Regional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEANERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

- ~~Complaint~~

Complaints

#### 1.4. Additional Compliance Information:

None



2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning Same-Day Operations	Medium	<p>The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8)</p> <p>OR</p> <p>The Responsible Entity has a</p>	<p>The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7)</p> <p>OR</p> <p>The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7)</p> <p>OR</p> <p>The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and</p>	<p>The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5)</p> <p>OR</p> <p>The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5)</p> <p>OR</p> <p>The Responsible Entity</p>	<p><u>The Responsible Entity did not document or implement physical security plans. (R1)</u></p> <p>OR</p> <p>The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1)</p> <p>OR</p> <p><u>The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1)</u></p> <p>OR</p> <p>The Responsible Entity</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified</del></p>	<p><del>identified deficiencies but did not assess or correct the deficiencies. (1.7)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)</del></p> <p><del>N/A</del></p>	<p><del>has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the</del></p>	<p><del>documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<del>deficiencies but did not assess or correct the deficiencies. (1.9)</del> OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9) <u>N/A</u>		<del>deficiencies. (1.6)</del> OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6) <u>N/A</u>	<del>correct the deficiencies. (1.2)</del> OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR <del>The Responsible Entity documented and</del>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p><del>implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity does not have a process</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4)</p> <p>OR</p> <p><del>The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)</del></p> <p>OR</p> <p><del>The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p><del>identify, assess, or correct the deficiencies. (1.4)</del></p> <p>OR</p> <p>The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical <del>security</del><u>Security</u> Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5)</p> <p>OR</p> <p>The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6)</p> <p>OR</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7)</p> <p>OR</p> <p>The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8)</p> <p>OR</p> <p>The Responsible Entity does not have a process to retain physical access logs for 90 calendar</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>days. (1.9)</p> <p><u>OR</u></p> <p><u>The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)</u></p>
R2	Same-Day Operations	Medium	N/A	<del>The Responsible Entity included a visitor control program that requires logging of each</del>	<del>The Responsible Entity included a visitor control program that requires continuous</del>	The Responsible Entity has failed to include or implement a visitor control program that



R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p><del>of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity included a visitor control program to retain visitor logs for at</del></p>	<p><del>escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)</del></p> <p><del>N/A</del></p>	<p>requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1)</p> <p>OR</p> <p>The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2)</p> <p>OR</p> <p>The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p><del>least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3)</del></p> <p>OR</p> <p><del>The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)</del> <u>N/A</u></p>		
<b>R3</b>	<b>Long Term Planning</b>	<b>Medium</b>	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity <del>has</del> <u>did</u> not <del>documented and implemented</del> <u>document or implement</u> a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

None.

**Version History**

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>1</u>	<u>1/16/06</u>	<u>R3.2 — Change “Control Center” to “control center.”</u>	<u>3/24/06</u>
<u>2</u>	<u>9/30/09</u>	<u>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</u> <u>Removal of reasonable business judgment.</u> <u>Replaced the RRO with the RE as a responsible entity.</u> <u>Rewording of Effective Date.</u> <u>Changed compliance monitor to Compliance Enforcement Authority.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Updated Version Number from -2 to -3</u> <u>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.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Approved by the NERC Board of Trustees.</u>	
<u>3</u>	<u>3/31/10</u>	<u>Approved by FERC.</u>	
<u>4</u>	<u>1/24/11</u>	<u>Approved by the NERC Board of</u>	

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
		<u>Trustees.</u>	
<u>5</u>	<u>11/26/12</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</u>
<u>5</u>	<u>11/22/13</u>	<u>FERC Order issued approving CIP-006-5.</u>	
<u>6</u>	<u>11/13/14</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Addressed FERC directives from Order No. 791.</u>

## 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~~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.

#### General:

While the focus ~~is of this Reliability Standard has~~ shifted away from the definition and management of a completely enclosed “six-wall” boundary, it is expected that in many instances ~~this a six-wall boundary~~ will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

#### Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, ~~a sole perimeter's~~ controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person ~~they are~~ the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, ~~1.76~~ and ~~1.87~~ beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be



implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

**Requirement R2:**

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

**Requirement R3:**

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

**Rationale:**

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts text boxes~~ were embedded within the standard ~~to explain the rationale for various parts of the standard.~~ Upon BOT approval, ~~that information~~ the text from the rationale text boxes was moved to this section.

**Rationale for Requirement R1:**

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, ~~1.76~~ and ~~1.87~~ beyond what is already required for the PSP.

~~**Summary of Changes:** The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.~~

~~Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.~~

~~Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.~~

~~**Reference to prior version:** (Part 1.1) CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity~~

~~**Change Rationale:** (Part 1.1)~~

~~To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.~~

~~**Reference to prior version:** (Part 1.2) CIP006-4c, R3 & R4~~

~~**Change Rationale:** (Part 1.2)~~

~~This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.~~

~~**Reference to prior version:** (Part 1.3) CIP006-4c, R3 & R4~~

~~**Change Rationale:** (Part 1.3)~~

~~The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.~~

~~Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.~~

~~FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).~~

~~**Reference to prior version:** (Part 1.4) CIP006-4c, R5~~

~~**Change Rationale:** (Part 1.4)~~

~~Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.~~

~~**Reference to prior version:** (Part 1.5) CIP006-4c, R5~~

~~**Change Rationale:** (Part 1.5)~~

~~Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.~~

~~Reference to prior version: (Part 1.6) CIP006-4c, R5~~

~~Change Rationale: (Part 1.6)~~

~~Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.~~

~~Reference to prior version: (Part 1.7) CIP006-4c, R5~~

~~Change Rationale: (Part 1.7)~~

~~Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.~~

~~Reference to prior version: (Part 1.8) CIP-006-4c, R6~~

~~Change Rationale: (Part 1.8)~~

~~CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.~~

~~Examples of logging methods have been moved to the Guidelines and Technical Basis section.~~

~~Reference to prior version: (Part 1.9) CIP-006-4c, R7~~

~~Change Rationale: (Part 1.9)~~

~~No change.~~

### **Rationale for R2:**

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

### **Rationale for Requirement R2:**

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

~~**Summary of Changes:** Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.~~

~~**Reference to prior version:** (Part 2.1) CIP-006-4c, R1.6.2~~

~~**Change Rationale:** (Part 2.1)~~

~~Added the ability to not do this during CIP Exceptional Circumstances.~~

~~**Reference to prior version:** (Part 2.2) CIP-006-4c R1.6.1~~

~~**Change Rationale:** (Part 2.2)~~

~~Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor the visitor. There is no requirement to document the escort or handoffs between escorts.~~

~~**Reference to prior version:** (Part 2.3) CIP-006-4c, R7~~

~~**Change Rationale:** (Part 2.3)~~

~~No change~~

**Rationale for Requirement R3:**

To ensure all Physical Access Control Systems and devices continue to function properly.

~~**Summary of Changes:** Reformatted into table structure.~~

~~Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.~~

~~**Reference to prior version:** (Part 3.1) CIP-006-4c, R8.1 and R8.2~~

~~**Change Rationale:** (Part 3.1)~~

~~Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.~~

**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	

Version	Date	Action	Change Tracking
		<p><del>elements of standards.</del></p> <p><del>Removal of reasonable business judgment.</del></p> <p><del>Replaced the RRO with the RE as a responsible entity.</del></p> <p><del>Rewording of Effective Date.</del></p> <p><del>Changed compliance monitor to Compliance Enforcement Authority.</del></p>	
<del>3</del>	<del>12/16/09</del>	<p><del>Updated Version Number from 2 to 3</del></p> <p><del>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.</del></p>	
<del>3</del>	<del>12/16/09</del>	<del>Approved by the NERC Board of Trustees.</del>	
<del>3</del>	<del>3/31/10</del>	<del>Approved by FERC.</del>	
<del>4</del>	<del>1/24/11</del>	<del>Approved by the NERC Board of Trustees.</del>	
<del>5</del>	<del>11/26/12</del>	<del>Adopted by the NERC Board of Trustees.</del>	<del>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</del>
<del>5</del>	<del>11/22/13</del>	<del>FERC Order issued approving CIP-006-5. (Order becomes effective on 2/3/14.)</del>	
<del>5</del>	<del>4/2/14</del>	<del>Address directive in FERC Order 791 to modify VRF in Requirement R3</del>	<del>VRF R3</del>

**Reliability Standard CIP-007-6 Clean and Redline**

## A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-6
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
    - 4.1.3 **Generator Operator**
    - 4.1.4 **Generator Owner**
    - 4.1.5 **Interchange Coordinator or Interchange Authority**
    - 4.1.6 **Reliability Coordinator**

**4.1.7 Transmission Operator**

**4.1.8 Transmission Owner**

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

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-007-6:

**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-002-5.1 identification and categorization processes.

**5. Effective Dates:**

See Implementation Plan for CIP-007-6.

**6. Background:**

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires 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 “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

## B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. [*Violation Risk Factor: Medium*] [*Time Horizon: Same Day Operations.*]
- M1.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R1– Ports and Services			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group.</li> <li>• Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or</li> <li>• Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.</li> </ul>

CIP-007-6 Table R1– Ports and Services			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. PCA; and</li> <li>2. Nonprogrammable communication components located inside both a PSP and an ESP.</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. PCA; and</li> <li>2. Nonprogrammable communication components located inside both a PSP and an ESP.</li> </ol>	<p>Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.</p>	<p>An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.</p>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. [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-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.</p>	<p>An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.</p>

CIP-007-6 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.</p>	<p>An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.</p>



CIP-007-6 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:</p> <ul style="list-style-type: none"> <li>• Apply the applicable patches; or</li> <li>• Create a dated mitigation plan; or</li> <li>• Revise an existing mitigation plan.</li> </ul> <p>Mitigation plans shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or</li> <li>• A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.</li> </ul>

CIP-007-6 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.</p>	<p>An example of evidence may include, but is not limited to, records of implementation of mitigations.</p>

- R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].
- M3.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Mitigate the threat of detected malicious code.	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records of response processes for malicious code detection</li> <li>• Records of the performance of these processes when malicious code is detected.</li> </ul>
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

- R4.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]
- M4.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:</p> <ol style="list-style-type: none"> <li>4.1.1. Detected successful login attempts;</li> <li>4.1.2. Detected failed access attempts and failed login attempts;</li> <li>4.1.3. Detected malicious code.</li> </ol>	<p>Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.</p>

CIP-007-6 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):</p> <ol style="list-style-type: none"> <li>4.2.1. Detected malicious code from Part 4.1; and</li> <li>4.2.2. Detected failure of Part 4.1 event logging.</li> </ol>	<p>Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.</p>

CIP-007-6 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.</p>	<p>Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.</p>
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.</p>	<p>Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.</p>

- R5.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].
- M5.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.



CIP-007-6 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Have a method(s) to enforce authentication of interactive user access, where technically feasible.</p>	<p>An example of evidence may include, but is not limited to, documentation describing how access is authenticated.</p>

CIP-007-6 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).</p>	<p>An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.</p>

CIP-007-6 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Change known default passwords, per Cyber Asset capability	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records of a procedure that passwords are changed when new devices are in production; or</li> <li>• Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.</li> </ul>

CIP-007-6 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:</p> <p>5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and</p> <p>5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or</li> <li>• Attestations that include a reference to the documented procedures that were followed.</li> </ul>

CIP-007-6 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.6	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or</li> <li>• Attestations that include a reference to the documented procedures that were followed.</li> </ul>

CIP-007-6 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.7	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, either:</p> <ul style="list-style-type: none"> <li>• Limit the number of unsuccessful authentication attempts; or</li> <li>• Generate alerts after a threshold of unsuccessful authentication attempts.</li> </ul>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Documentation of the account-lockout parameters; or</li> <li>• Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.</li> </ul>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Additional Compliance Information:

None



**2. Table of Compliance Elements**

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R1</b>	<b>Same Day Operations</b>	<b>Medium</b>	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)
<b>R2</b>	<b>Operations Planning</b>	<b>Medium</b>	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-6 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R3</b>	<b>Same Day Operations</b>	<b>Medium</b>	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2)  OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3).  OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R4</b>	<b>Same Day Operations and Operations Assessment</b>	<b>Medium</b>	<p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)</p>	<p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)</p>	<p>The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in</p>	<p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (R4)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but</p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
<b>R5</b>	<b>Operations Planning</b>	<b>Medium</b>	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2)  OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5)  OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5)</p> <p>OR</p>	<p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change</p>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or</p>	<p>known default passwords. (5.4)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6)  OR  The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

**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.	

Version	Date	Action	Change Tracking
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.
5	11/22/13	FERC Order issued approving CIP-007-5.	
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	2/15/15	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.

## 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:**

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible (“listening”) ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset’s function, and disable or restrict access to all other ports.

**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP\_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed ‘needed.’

**1.2.** Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for ‘console commands’ primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

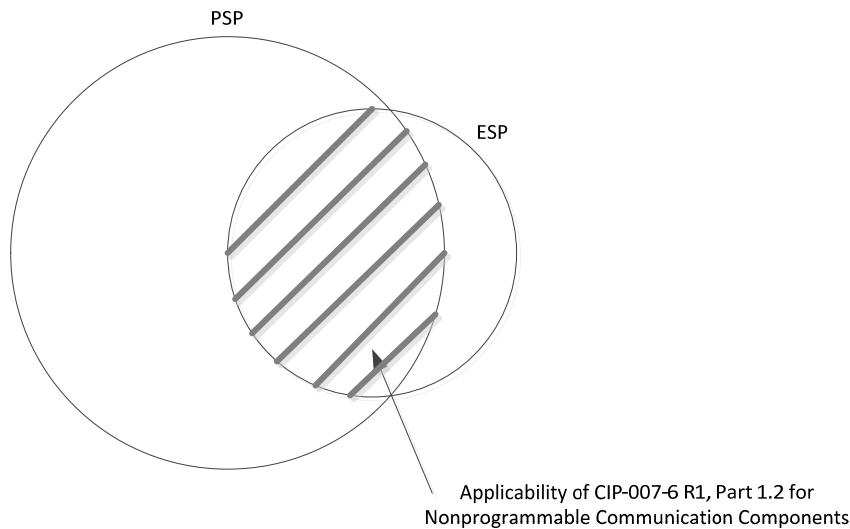
- Disabling all unneeded physical ports within the Cyber Asset’s configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a ‘defense in depth’ type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to “think before you plug anything into one of these systems” which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include “Nonprogrammable communication components located inside both a PSP and an ESP.” This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

**Location of Nonprogrammable Communication Components**



**Requirement R2:**

The SDT’s intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an “install every security patch” requirement; the main intention is to “be aware of in a timely manner and manage all known vulnerabilities” requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they



can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

### **Requirement R3:**

**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System’s ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a ‘false positive’ could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

### **Requirement R4:**

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-

time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

**Requirement R5:**

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

**5.1** Reference the Requirement's rationale.

**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, \$, @, &), in various combinations.

**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

## **Rationale:**

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

### **Rationale for Requirement R1:**

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

### **Rationale for Requirement R2:**

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

### **Rationale for Requirement R3:**

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

### **Rationale for Requirement R4:**

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

### **Rationale for Requirement R5:**

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.



The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

## A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-~~56~~
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the ~~BES~~ Bulk Electric System (BES).
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

**4.2.1.2** Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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-007-~~56~~:

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

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

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

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

**4.2.3.5** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. ~~5.~~ Effective Dates:**

~~1. 24 Months Minimum — CIP 007 5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP 007 5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~See Implementation Plan for CIP-007-6.~~

**6. Background:**

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

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

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

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

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

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

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

Measures 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-BES~~. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

**“Applicable Systems” Columns in Tables:**

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

## B. Requirements and Measures

- R1.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~56~~ Table R1 – Ports and Services*. [*Violation Risk Factor: Medium*] [*Time Horizon: Same Day Operations.*]
- M1.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~56~~ Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-56 Table R1– Ports and Services			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group.</li> <li>• Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or</li> <li>• Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.</li> </ul>



CIP-007-56 Table R1– Ports and Services			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems <u>and their associated:</u></p> <ol style="list-style-type: none"> <li>1. <u>PCA; and</u></li> <li>2. <u>Nonprogrammable communication components located inside both a PSP and an ESP.</u></li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers <u>and their associated:</u></p> <ol style="list-style-type: none"> <li>1. <u>PCA; and</u></li> <li>2. <u>Nonprogrammable communication components located inside both a PSP and an ESP.</u></li> </ol>	<p>Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or <del>removable media</del> <u>Removable Media.</u></p>	<p>An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.</p>

- R2.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~ process(es) that collectively include each of the applicable requirement parts in *CIP-007-56 Table R2 – Security Patch Management*. [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-007-56 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-56 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.</p>	<p>An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.</p>

CIP-007-56 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.</p>	<p>An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.</p>

CIP-007-56 Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:</p> <ul style="list-style-type: none"> <li>• Apply the applicable patches; or</li> <li>• Create a dated mitigation plan; or</li> <li>• Revise an existing mitigation plan.</li> </ul> <p>Mitigation plans shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or</li> <li>• A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.</li> </ul>

**CIP-007-56 Table R2 – Security Patch Management**

Part	Applicable Systems	Requirements	Measures
2.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.</p>	<p>An example of evidence may include, but is not limited to, records of implementation of mitigations.</p>

- R3.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~ process(es) that collectively include each of the applicable requirement parts in *CIP-007-56 Table R3 – Malicious Code Prevention*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].
- M3.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-56 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-56 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-56 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Mitigate the threat of detected malicious code.	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records of response processes for malicious code detection</li> <li>• Records of the performance of these processes when malicious code is detected.</li> </ul>
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

- R4.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~ process(es) that collectively include each of the applicable requirement parts in *CIP-007-56 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*
- M4.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-56 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-56 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: <ol style="list-style-type: none"> <li>4.1.1. Detected successful login attempts;</li> <li>4.1.2. Detected failed access attempts and failed login attempts;</li> <li>4.1.3. Detected malicious code.</li> </ol>	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.



**CIP-007-56 Table R4 – Security Event Monitoring**

Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):</p> <ol style="list-style-type: none"> <li>4.2.1. Detected malicious code from Part 4.1; and</li> <li>4.2.2. Detected failure of Part 4.1 event logging.</li> </ol>	<p>Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.</p>

**CIP-007-56 Table R4 – Security Event Monitoring**

Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.</p>	<p>Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.</p>
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	<p>Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.</p>	<p>Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.</p>

- R5.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~56~~ Table R5 – System Access Controls*. [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].
- M5.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~56~~ Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-56 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Have a method(s) to enforce authentication of interactive user access, where technically feasible.</p>	<p>An example of evidence may include, but is not limited to, documentation describing how access is authenticated.</p>

CIP-007-56 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).</p>	<p>An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.</p>

CIP-007-56 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Identify individuals who have authorized access to shared accounts.</p>	<p>An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.</p>

CIP-007-56 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Change known default passwords, per Cyber Asset capability	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records of a procedure that passwords are changed when new devices are in production; or</li> <li>• Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.</li> </ul>

CIP-007-56 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:</p> <p>5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and</p> <p>5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or</li> <li>• Attestations that include a reference to the documented procedures that were followed.</li> </ul>



CIP-007-56 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.6	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or</li> <li>• Attestations that include a reference to the documented procedures that were followed.</li> </ul>

CIP-007-56 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.7	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Where technically feasible, either:</p> <ul style="list-style-type: none"> <li>• Limit the number of unsuccessful authentication attempts; or</li> <li>• Generate alerts after a threshold of unsuccessful authentication attempts.</li> </ul>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Documentation of the account-lockout parameters; or</li> <li>• Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.</li> </ul>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority (~~“ (CEA)” unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEANERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Violation Investigations

Self-Reporting

• ~~Complaint~~

Complaints

#### 1.4. Additional Compliance Information:

None

~~D. Regional Variances~~

None.

~~E. Interpretations~~

None.

~~F. Associated Documents~~

None.

---

---

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)				
			Lower VSL	Moderate VSL	High VSL	Severe VSL	
R1	Same Day Operations	Medium	N/A	<p>The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or <del>removable media and has identified deficiencies but did not assess or correct the deficiencies.</del><u>Removable Media.</u> (1.2)</p> <p>OR</p> <p><del>The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical</del></p>	<p>The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (1.1)</p> <p>OR</p> <p>The Responsible Entity has implemented and documented processes for</p>	<p>The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (1.1)</p> <p>OR</p> <p>The Responsible Entity has implemented and documented processes for</p>	<p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in <del>CIP-007-5 Table R1 and has identified deficiencies but did not assess or correct the deficiencies.</del><u>6 Table R1.</u> (R1)</p> <p>OR</p> <p><del>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<del>input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)</del>	<del>determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)</del>	<del>the deficiencies. (R1)</del>
<b>R2</b>	<b>Operations Planning</b>	<b>Medium</b>	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets <del>and has identified deficiencies but did not</del>	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets <del>and has identified</del>	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 <del>and has identified deficiencies but did not assess or correct the</del>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>but less than 50 calendar days of the last evaluation for the source or sources identified <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for</p>	<p><del>assess or correct the deficiencies.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for</p>	<p><del>deficiencies but did not assess or correct the deficiencies.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one</p>	<p><del>deficiencies.</del> Table R2. (R2)</p> <p>OR</p> <p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2)</p> <p>OR</p> <p>The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating,</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)</del></p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50</p>	<p>applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified <del>and has identified deficiencies but did not assess or correct the deficiencies. (2.2)</del></p> <p>OR</p> <p><del>The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days</del></p>	<p>or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified <del>and has identified deficiencies but did not assess or correct the deficiencies. (2.2)</del></p> <p>OR</p> <p><del>The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did</del></p>	<p>or installing cyber security patches for applicable Cyber Assets <del>and has identified deficiencies but did not assess or correct the deficiencies. (2.1)</del></p> <p>OR</p> <p><del>The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or</del></p>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>calendar days of the evaluation completion <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (2.3)</p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35</p>	<p><del>of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion <del>and has identified deficiencies</del></p>	<p><del>not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation</p>	<p><del>correct the deficiencies.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (2.4)</p> <p>OR</p> <p>The Responsible Entity documented a mitigation plan</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)</del></p>	<p><del>but did not assess or correct the deficiencies. (2.3)</del></p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or</p>	<p>plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3)</p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not</p>	<p><del>for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4)</del></p> <p>OR</p> <p>The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<del>correct the deficiencies. (2.3)</del>	<del>patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)</del>	<del>not assess or correct the deficiencies. (2.4)</del>  <del>OR</del> <del>The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)</del>
R3	Same Day Operations	Medium	<u>N/A</u>	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns	The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>are used, the Responsible Entity did not address testing the signatures or patterns <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (3.3)</p> <p>OR</p> <p><del>The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies.</del> (3.3)</p>	<p>malicious code prevention but did not mitigate the threat of detected malicious code <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (3.2)</p> <p>OR</p> <p><del>The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies.</del> (3.2)</p>	<p>that included the applicable items in CIP-007-5 <del>Table R3 and has identified deficiencies but did not assess or correct the deficiencies.</del> (R3) <del>Table R3.</del> (R3).</p> <p>OR</p> <p><del>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify, assess, or correct the deficiencies.</del> (R3)</p> <p>OR</p> <p>The Responsible Entity has implemented one</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>OR</del></p> <p>The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections <del>and has identified deficiencies but did not assess or correct the deficiencies. (3.1)</del></p> <p><del>OR</del></p> <p>The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and</p>	<p>or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code <del>and has identified deficiencies but did not assess or correct the deficiencies. (3.1)</del></p> <p><del>OR</del></p> <p>The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<del>process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3). (3.3).</del>	<del>did not identify, assess, or correct the deficiencies. (3.1)</del>
<b>R4</b>	<b>Same Day Operations and Operations Assessment</b>	<b>Medium</b>	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and has identified deficiencies but did not assess or correct the deficiencies. 6 Table R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>days but missed an interval and completed the review within 22 calendar days of the prior review <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (4.4)</p> <p><del>OR</del></p> <p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed an</p>	<p>within 30 calendar days of the prior review <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (4.4)</p> <p><del>OR</del></p> <p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or</p>	<p>not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (4.2)</p> <p><del>OR</del></p> <p>The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the</p>	<p><del>OR</del></p> <p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)</p> <p><del>OR</del></p> <p>The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)</del></p>	<p><del>correct the deficiencies. (4.4)</del></p>	<p><del>required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2)</del></p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days <del>and has identified deficiencies but did</del></p>	<p>types of events described in 4.1.1 through 4.1.3 <del>and has identified deficiencies but did not assess or correct the deficiencies. (4.1)</del></p> <p>OR</p> <p><del>The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct</del></p>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>not assess or correct the deficiencies. (4.3)</del></p> <p>OR</p> <p><del>The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP-Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3)</del></p> <p>OR</p>	<p><del>the deficiencies. (4.1)</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals <del>and has identified deficiencies but did not assess or correct the deficiencies. (4.4)</del></p> <p>OR</p> <p><del>The Responsible Entity has documented and implemented one</del></p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<del>or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4). (4.4)</del>	
<b>R5</b>	<b>Operations Planning</b>	<b>Medium</b>	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R5 and has identified deficiencies but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (5.6)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for</p>	<p>an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (5.6)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change</p>	<p>inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled</p>	<p><del>not assess or correct the deficiencies.</del> <u>Table R5.</u> (R5)</p> <p>OR</p> <p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in <u>CIP-007-5 Table R5</u> and did not identify, assess, or correct the deficiencies. (R5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)</del></p>	<p><del>and did not identify, assess, or correct the deficiencies. (5.6)</del></p>	<p><del>default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2)</del></p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts <del>and has identified deficiencies but did</del></p>	<p>technically feasible, does not have a method(s) to enforce authentication of interactive user access <del>and has identified deficiencies but did not assess or correct the deficiencies. (5.1)</del></p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>not assess or correct the deficiencies. (5.3)</del></p> <p>OR</p> <p><del>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)</del></p> <p>OR</p> <p>The Responsible Entity has implemented one or more</p>	<p><del>access and did not identify, assess, or correct the deficiencies. (5.1)</del></p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4)</p> <p>OR</p> <p><del>The Responsible Entity has implemented one</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (5.5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for</p>	<p><del>or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies.</del> (5.4)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 <del>and did not identify, assess, or correct the deficiencies.</del> (5.5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an</p>	<p>password parameters described in 5.5.1 and 5.5.2 <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (5.5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1</p>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change <del>and has identified deficiencies but did not assess or correct the deficiencies.</del> (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally	<del>and 5.5.2 and did not identify, assess, or correct the deficiencies.</del> (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change <del>and has identified deficiencies but did</del>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)</del></p>	<p><del>not assess or correct the deficiencies. (5.6)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p><del>correct the deficiencies.</del> (5.6)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts <del>and has identified deficiencies but did not assess or</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p><del>correct the deficiencies. (5.7)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7).</del></p> <p><u>(5.7)</u></p>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>1</u>	<u>1/16/06</u>	<u>R3.2 — Change “Control Center” to “control center.”</u>	<u>3/24/06</u>
<u>2</u>	<u>9/30/09</u>	<u>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</u> <u>Removal of reasonable business judgment.</u> <u>Replaced the RRO with the RE as a responsible entity.</u> <u>Rewording of Effective Date.</u> <u>Changed compliance monitor to Compliance Enforcement Authority.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Updated Version Number from -2 to -3</u> <u>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.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Approved by the NERC Board of Trustees.</u>	
<u>3</u>	<u>3/31/10</u>	<u>Approved by FERC.</u>	

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>4</u>	<u>1/24/11</u>	<u>Approved by the NERC Board of Trustees.</u>	
<u>5</u>	<u>11/26/12</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</u>
<u>5</u>	<u>11/22/13</u>	<u>FERC Order issued approving CIP-007-5.</u>	
<u>6</u>	<u>11/13/14</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.</u>
<u>6</u>	<u>2/15/15</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>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.</u>

## 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-~~5-5.1’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:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible (“listening”) ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset’s function, and disable or restrict access to all other ports.

**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP\_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed ‘needed.’

**1.2.** Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

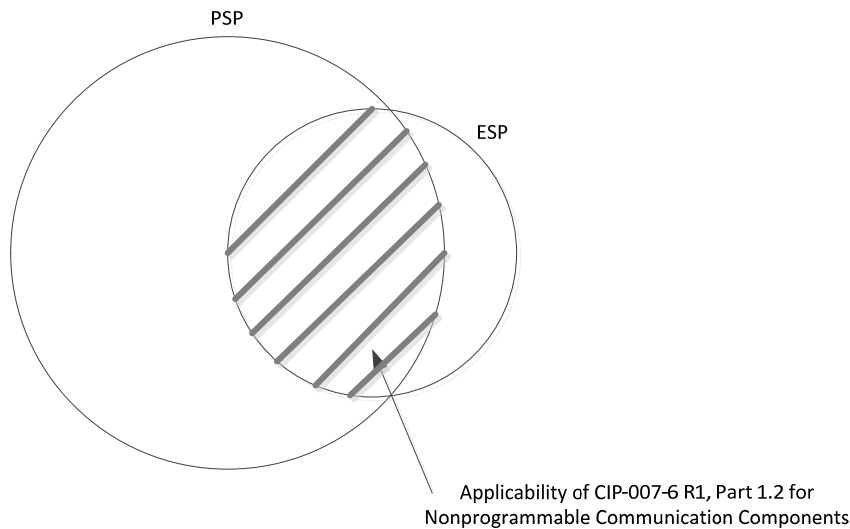
The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense ~~are~~is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



### Location of Nonprogrammable Communication Components



### Requirement R2:

The SDT’s intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an “install every security patch” requirement; the main intention is to “be aware of in a timely manner and manage all known vulnerabilities” requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. ~~Stand-alone~~Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

### **Requirement R3:**

**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, ~~portable storage media policies,~~ Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System’s ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a ‘false positive’ could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

**Requirement R4:**

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of ~~removable media~~ Removable Media in violation of a policy

**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-

time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

**Requirement R5:**

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

**5.1** Reference the Requirement's rationale.

**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, \$, @, &), in various combinations.

**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

## Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts text boxes~~ were embedded within the standard ~~to explain the rationale for various parts of the standard.~~ Upon BOT approval, ~~that information~~ the text from the rationale text boxes was moved to this section.

### Rationale for **Requirement R1**:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

~~**Summary of Changes:** Changed the ‘needed for normal or emergency operations’ to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.~~

~~**Reference to prior version:** (Part 1.1) CIP-007-4, R2.1 and R2.2~~

~~**Change Rationale:** (Part 1.1)~~

~~*The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of ‘normal or emergency’ added no value and has been removed.*~~

~~**Reference to prior version:** (Part 1.2) New~~

~~**Change Rationale:** (Part 1.2)~~

~~*On March 18, 2010, FERC issued an order to approve NERC’s interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term “ports” in “ports and services” refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*~~

In response to FERC Order No. 791, specifically FERC’s reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity’s control (i.e. as part of the telecommunication carrier’s network).

### Rationale for **Requirement R2**:



Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

~~The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.~~

~~**Summary of Changes:** The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the “release” date was. The current wording stated “document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades” and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.~~

~~**Reference to prior version:** (Part 2.1) CIP-007, R3~~

~~**Change Rationale:** (Part 2.1)~~

~~The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.~~

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

~~**Change Rationale:** (Part 2.2)~~

~~Similar to the current wording but added “from the source or sources identified in 2.1” to clarify the 35-day time frame.~~

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

~~**Change Rationale:** (Part 2.3)~~

~~The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.~~

~~**Reference to prior version:** (Part 2.4) CIP-007, R3.2~~

~~**Change Rationale:** (Part 2.4)~~

~~Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.~~

**Rationale for Requirement R3:**

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

**Summary of Changes:** ~~In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.~~

~~Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method...However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance..."~~

~~In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.~~

~~**Reference to prior version:** (Part 3.1) CIP-007-4, R4; CIP-007-4, R4.1~~

~~**Change Rationale:** (Part 3.1)~~

~~See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.~~

~~**Reference to prior version:** (Part 3.2) CIP-007-4, R4; CIP-007-4, R4.1~~

~~**Change Rationale:** (Part 3.2)~~

~~See the Summary of Changes.~~

~~**Reference to prior version:** (Part 3.3) CIP-007-4, R4; CIP-007-4, R4.2~~

~~**Change Rationale:** (Part 3.3)~~

~~**Requirement** essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.~~

**Rationale for Requirement R4:**

**Rationale for R4:** Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

~~**Summary of Changes:** Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor.”~~

~~The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.~~

~~In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.~~

~~**Reference to prior version:** (Part 4.1) CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3~~

~~**Change Rationale:** (Part 4.1)~~

~~This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.~~

~~**Reference to prior version:** (Part 4.2) CIP-005-4, R3.2; CIP-007-4, R6.2~~

~~**Change Rationale:** (Part 4.2)~~

~~This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.~~

~~Reference to prior version: (Part 4.3) CIP-005-4, R3.2; CIP-007-4, R6.4~~

~~Change Rationale: (Part 4.3)~~

~~No substantive change.~~

~~Reference to prior version: (Part 4.4) CIP-005-4, R3.2; CIP-007-4, R6.5~~

~~Change Rationale: (Part 4.4)~~

~~Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.~~

#### **Rationale for Requirement R5:**

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to

make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts

for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

**Summary of Changes (From R5):**

~~CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.~~

~~Reference to prior version: (Part 5.1) CIP-007-4, R5~~

~~Change Rationale: (Part 5.1)~~

~~The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase “that minimize the risk of unauthorized access” was removed and more appropriately captured in the rationale statement.~~

~~Reference to prior version: (Part 5.2) CIP-007-4, R5.2 and R5.2.1~~

~~Change Rationale: (Part 5.2)~~

~~CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.~~

~~Reference to prior version: (Part 5.3) CIP-007-4, R5.2.2~~

~~Change Rationale: (Part 5.3)~~

~~No significant changes. Added “authorized” access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.~~

~~Reference to prior version: (Part 5.4) CIP-007-4, R5.2.1~~

~~Change Rationale: (Part 5.4)~~

~~The requirement for the “removal, disabling or renaming of such accounts where possible” has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of~~

~~having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.~~

~~Reference to prior version: (Part 5.5) CIP-007-4, R5.3~~

~~Change Rationale: (Part 5.5)~~

~~CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.~~

~~Reference to prior version: (Part 5.6) CIP-007-4, R5.3.3~~

~~Change Rationale: (Part 5.6)~~

~~\*This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.~~

~~Reference to prior version: (Part 5.7) New Requirement~~

~~Change Rationale: (Part 5.7)~~

~~Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.~~

### 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	

		<p><del>with the latest guidelines for developing compliance elements of standards.</del></p> <p><del>Removal of reasonable business judgment.</del></p> <p><del>Replaced the RRO with the RE as a responsible entity.</del></p> <p><del>Rewording of Effective Date.</del></p> <p><del>Changed compliance monitor to Compliance Enforcement Authority.</del></p>	
3	12/16/09	<p><del>Updated version number from 2 to 3</del></p> <p><del>Approved by the NERC Board of Trustees.</del></p>	
3	3/31/10	<p><del>Approved by FERC.</del></p>	
4	12/30/10	<p><del>Modified to add specific criteria for Critical Asset identification.</del></p>	Update
4	1/24/11	<p><del>Approved by the NERC Board of Trustees.</del></p>	Update
5	11/26/12	<p><del>Adopted by the NERC Board of Trustees.</del></p>	<p><del>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</del></p>
5	11/22/13	<p><del>FERC Order issued approving CIP-007-5. (Order becomes effective on 2/3/14.)</del></p>	



**Reliability Standard CIP-009-6 Clean and Redline**

## A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems
2. **Number:** CIP-009-6
3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
    - 4.1.3 **Generator Operator**
    - 4.1.4 **Generator Owner**
    - 4.1.5 **Interchange Coordinator or Interchange Authority**
    - 4.1.6 **Reliability Coordinator**

**4.1.7 Transmission Operator**

**4.1.8 Transmission Owner**

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

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-009-6:

**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-002-5.1 identification and categorization processes.

**5. Effective Dates:**

See Implementation Plan for CIP-009-6.

**6. Background:**

Standard CIP-009 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 their documented processes, but they 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 “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and 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 include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

**B. Requirements and Measures**

- R1.** Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
- M1.** Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.</p>	<p>An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.</p>
1.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.</p>	<p>An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.</p>



- R2.** Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery 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-009-6 Table R2 – Recovery Plan Implementation and Testing*.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months:</p> <ul style="list-style-type: none"> <li>• By recovering from an actual incident;</li> <li>• With a paper drill or tabletop exercise; or</li> <li>• With an operational exercise.</li> </ul>	<p>An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.</p>

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.</p> <p>An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.</p>	<p>An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).</p>
2.3	High Impact BES Cyber Systems	<p>Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.</p> <p>An actual recovery response may substitute for an operational exercise.</p>	<p>Examples of evidence may include, but are not limited to, dated documentation of:</p> <ul style="list-style-type: none"> <li>• An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or</li> <li>• An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.</li> </ul>

- R3.** Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Assessment*].
- M3.** Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>No later than 90 calendar days after completion of a recovery plan test or actual recovery:</p> <ol style="list-style-type: none"> <li>3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;</li> <li>3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and</li> <li>3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.</li> </ol>	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned;</li> <li>2. Dated and revised recovery plan showing any changes based on the lessons learned; and</li> <li>3. Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> <li>• Emails;</li> <li>• USPS or other mail service;</li> <li>• Electronic distribution system; or</li> <li>• Training sign-in sheets.</li> </ul> </li> </ol>

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:</p> <ol style="list-style-type: none"> <li>3.2.1. Update the recovery plan; and</li> <li>3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.</li> </ol>	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and</li> <li>2. Evidence of plan update distribution including, but not limited to:                             <ul style="list-style-type: none"> <li>• Emails;</li> <li>• USPS or other mail service;</li> <li>• Electronic distribution system; or</li> <li>• Training sign-in sheets.</li> </ul> </li> </ol>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

#### 1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R1</b>	<b>Long-term Planning</b>	<b>Medium</b>	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems.  OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1.  OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R2</b>	<b>Operations Planning</b> <b>Real-time Operations</b>	<b>Lower</b>	<p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested</p>	<p>The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan</p>	<p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested</p>	<p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months</p>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
<b>R3</b>	<b>Operations Assessment</b>	<b>Lower</b>	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	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 each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) <ul style="list-style-type: none"> <li>• Roles or responsibilities, or</li> <li>• Responders, or</li> <li>• Technology changes.</li> </ul>	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery 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 determines would impact the ability to execute the plan: (3.2) <ul style="list-style-type: none"> <li>• Roles or responsibilities, or</li> <li>• Responders, or</li> <li>• Technology changes.</li> </ul>	

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

None.

**Version History**

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

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791

## Guidelines and Technical Basis

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

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

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

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

#### Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at <http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf>
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf)

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

### **Requirement R2:**

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

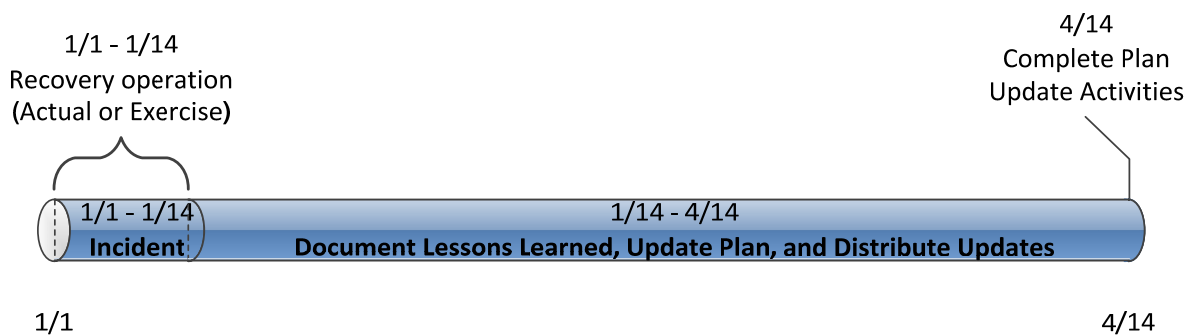
The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

**Requirement R3:**

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.



**Figure 1: CIP-009-6 R3 Timeline**

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.



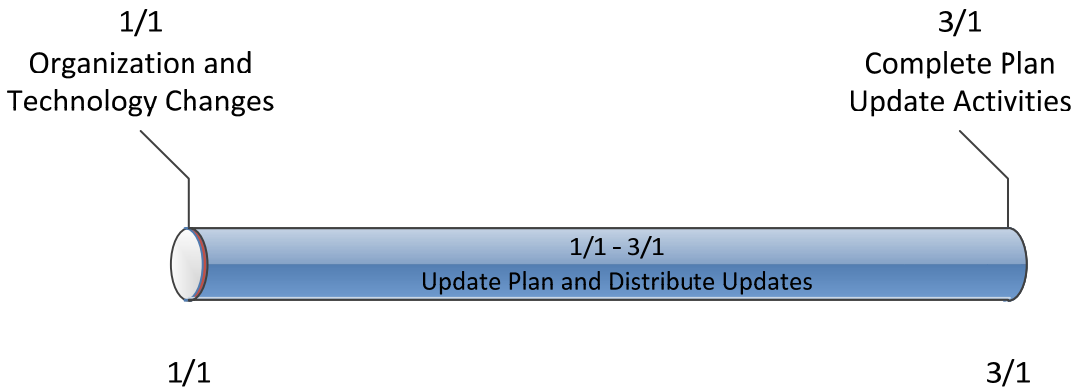


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

**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:**

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

**Rationale for Requirement R2:**

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

**Rationale for Requirement R3:**

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

## A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems
2. **Number:** CIP-009-~~56~~
3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
    - 4.1.3 **Generator Operator**
    - 4.1.4 **Generator Owner**
    - 4.1.5 **Interchange Coordinator or Interchange Authority**
    - 4.1.6 **Reliability Coordinator**

**4.1.7 Transmission Operator**

**4.1.8 Transmission Owner**

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

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-009-56:

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

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

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

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

**4.2.3.5** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. ~~5.~~ Effective Dates:**

~~1. **24 Months Minimum**—CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~See Implementation Plan for CIP-009-6.~~

**6. Background:**

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

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

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

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the "... identifies, assesses, and corrects deficiencies, ..." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

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

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

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

Measures 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-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and 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 include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

**B. Requirements and Measures**

- R1.** Each Responsible Entity shall have one or more documented recovery ~~plans~~plan(s) that collectively include each of the applicable requirement parts in CIP-009-56 Table R1 – Recovery Plan Specifications. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
- M1.** Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in CIP-009-56 Table R1 – Recovery Plan Specifications.

CIP-009-56 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).



CIP-009-56 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-56 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.</p>	<p>An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.</p>
1.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.</p>	<p>An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.</p>

- R2.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-56 Table R2 – Recovery 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-009-56 Table R2 – Recovery Plan Implementation and Testing*.

CIP-009-56 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> Medium Impact BES Cyber Systems at Control Centers and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: <ul style="list-style-type: none"> <li>• By recovering from an actual incident;</li> <li>• With a paper drill or tabletop exercise; or</li> <li>• With an operational exercise.</li> </ul>	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-56 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.</p> <p>An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.</p>	<p>An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).</p>
2.3	High Impact BES Cyber Systems	<p>Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.</p> <p>An actual recovery response may substitute for an operational exercise.</p>	<p>Examples of evidence may include, but are not limited to, dated documentation of:</p> <ul style="list-style-type: none"> <li>• An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or</li> <li>• An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.</li> </ul>

- R3.** Each Responsible Entity shall maintain each of its recovery ~~plans~~plan(s) in accordance with each of the applicable requirement parts in *CIP-009-~~56~~ Table R3 – Recovery Plan Review, Update and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-~~56~~ Table R3 – Recovery Plan Review, Update and Communication*.

CIP-009-56 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>No later than 90 calendar days after completion of a recovery plan test or actual recovery:</p> <ol style="list-style-type: none"> <li>3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;</li> <li>3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and</li> <li>3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.</li> </ol>	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned;</li> <li>2. Dated and revised recovery plan showing any changes based on the lessons learned; and</li> <li>3. Evidence of plan update distribution including, but not limited to:                             <ul style="list-style-type: none"> <li>• Emails;</li> <li>• USPS or other mail service;</li> <li>• Electronic distribution system; or</li> <li>• Training sign-in sheets.</li> </ul> </li> </ol>

CIP-009-56 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:</p> <ol style="list-style-type: none"> <li>3.2.1. Update the recovery plan; and</li> <li>3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.</li> </ol>	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> <li>1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and</li> <li>2. Evidence of plan update distribution including, but not limited to:                             <ul style="list-style-type: none"> <li>• Emails;</li> <li>• USPS or other mail service;</li> <li>• Electronic distribution system; or</li> <li>• Training sign-in sheets.</li> </ul> </li> </ol>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority (~~“(“ (CEA”) unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. ~~In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

• ~~Complaint~~

Complaints

#### 1.4. Additional Compliance Information:

None



2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	<p>The Responsible Entity has not created recovery plan(s) for BES Cyber Systems.</p> <p>OR</p> <p>The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1.</p> <p>OR</p> <p>The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning Real-time Operations	Lower	<p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, <del>and when tested, any deficiencies were identified, assessed, and corrected.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, <del>and</del></p>	<p>The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, <del>and when tested, any deficiencies were identified, assessed, and corrected.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, <del>and when tested, any</del></p>	<p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, <del>and when tested, any deficiencies were identified, assessed, and corrected.</del> (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, <del>and</del></p>	<p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1)</p> <p>OR</p> <p><del>The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1)</del></p> <p>OR</p> <p><del>The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>when tested, any deficiencies were identified, assessed, and corrected.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, <del>and when tested, any deficiencies were identified, assessed, and corrected.</del> (2.3). (2.3)</p>	<p><del>deficiencies were identified, assessed, and corrected.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, <del>and when tested, any deficiencies were identified, assessed, and corrected.</del> (2.3). (2.3)</p>	<p><del>when tested, any deficiencies were identified, assessed, and corrected.</del> (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, <del>and when tested, any deficiencies were identified, assessed, and corrected.</del> (2.3). (2.3)</p>	<p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2)</p> <p>OR</p> <p><del>The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies.</del> (2.2)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p><del>OR</del></p> <p><del>The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)</del></p> <p><del>OR</del></p> <p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)</p> <p><del>OR</del></p> <p><del>The Responsible Entity has tested the recovery plan(s) according to R2 Part</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p><del>2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)</del></p>
<b>R3</b>	<b>Operations Assessment</b>	<b>Lower</b>	<p>The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)</p>	<p>The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2)</p> <p>OR</p>	<p>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 each recovery plan test or actual recovery. (3.1.1)</p>	<p>The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3)</p> <p>OR</p> <p>The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days 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"> <li>• Roles or responsibilities, or</li> <li>• Responders, or</li> </ul>	<p>OR</p> <p>The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2)</p> <p>OR</p> <p>The Responsible Entity has not updated the recovery 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 determines would impact the ability to execute the plan: (3.2)</p> <ul style="list-style-type: none"> <li>• Roles or responsibilities, or</li> </ul>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009- <del>56</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<ul style="list-style-type: none"> <li>• Technology changes.</li> </ul>	<ul style="list-style-type: none"> <li>• Responders, or <del>•</del> Technology changes.</li> </ul>	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>1</u>	<u>1/16/06</u>	<u>R3.2 — Change “Control Center” to “control center.”</u>	<u>3/24/06</u>
<u>2</u>	<u>9/30/09</u>	<u>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</u> <u>Removal of reasonable business judgment.</u> <u>Replaced the RRO with the RE as a responsible entity.</u> <u>Rewording of Effective Date.</u> <u>Changed compliance monitor to Compliance Enforcement Authority.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Updated Version Number from -2 to -3</u> <u>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.</u>	
<u>3</u>	<u>12/16/09</u>	<u>Approved by the NERC Board of Trustees.</u>	
<u>3</u>	<u>3/31/10</u>	<u>Approved by FERC.</u>	
<u>4</u>	<u>1/24/11</u>	<u>Approved by the NERC Board of Trustees.</u>	



<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>5</u>	<u>11/26/12</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</u>
<u>5</u>	<u>11/22/13</u>	<u>FERC Order issued approving CIP-009-5.</u>	
<u>6</u>	<u>11/13/14</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Addressed FERC directives from Order No. 791</u>

## 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-~~5-5.1's~~ categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

#### Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at <http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf>
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf)

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power ~~plants' facilities~~plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

### **Requirement R2:**

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

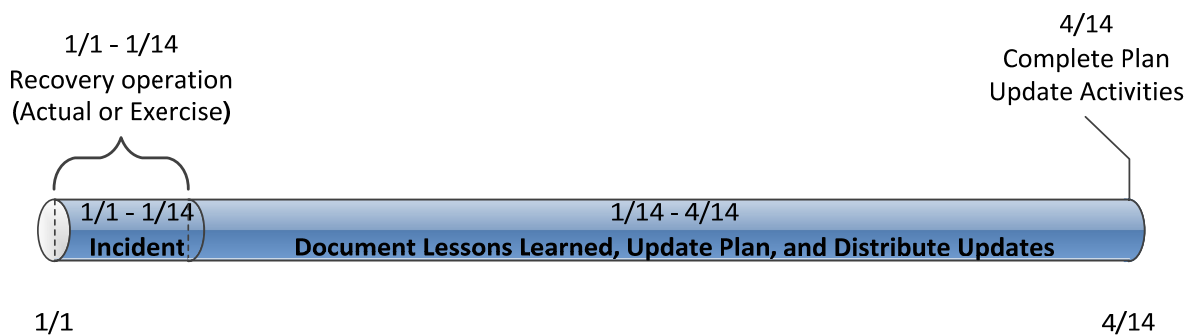
The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

**Requirement R3:**

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in ~~Figure 1~~ **Figure 1**, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.



**Figure 1: CIP-009-56 R3 Timeline**

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in ~~Figure 2~~ **Figure 2**, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

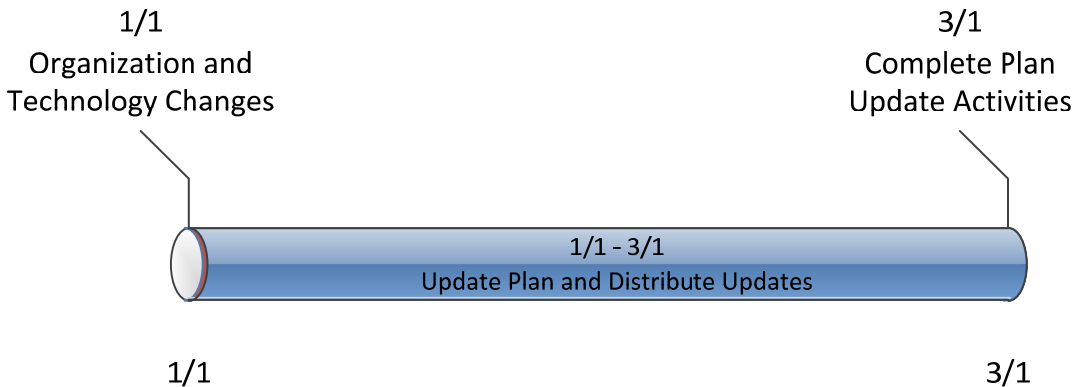


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

**Rationale:**

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts text boxes~~ were embedded within the standard ~~to explain the rationale for various parts of the standard.~~ Upon BOT approval, ~~that information~~ ~~the text from the rationale text boxes~~ was moved to this section.

**Rationale for Requirement R1:**

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

~~Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.~~

~~Reference to prior version: (Part 1.1) CIP-009, R1.1~~

~~Change Description and Justification: (Part 1.1)  
Minor wording changes; essentially unchanged.~~

~~Reference to prior version: (Part 1.2) CIP-009, R1.2~~

~~Change Description and Justification: (Part 1.2)  
Minor wording changes; essentially unchanged.~~

~~Reference to prior version: (Part 1.3) CIP-009, R4~~

~~Change Description and Justification: (Part 1.3)~~

~~Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.~~

~~Reference to prior version: (Part 1.4) New Requirement~~

~~Change Description and Justification: (Part 1.4)~~

~~Addresses FERC Order Section 739 and 748.~~

~~Reference to prior version: (Part 1.5) New Requirement~~

~~Change Description and Justification: (Part 1.5)~~

~~Added requirement to address FERC Order No. 706, Paragraph 706.~~

**Rationale for Requirement R2:**

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

~~**Summary of Changes:** Added operational testing for recovery of BES Cyber Systems.~~

~~**Reference to prior version:** (Part 2.1) CIP-009, R2~~

~~**Change Description and Justification:** (Part 2.1)~~

~~Minor wording change; essentially unchanged.~~

~~**Reference to prior version:** (Part 2.2) CIP-009, R5~~

~~**Change Description and Justification:** (Part 2.2)~~

~~Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.~~

~~**Reference to prior version:** (Part 2.3) CIP-009, R2~~

~~**Change Description and Justification:** (Part 2.3)~~

~~Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.~~

### **Rationale for Requirement R3:**

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

~~**Summary of Changes:** Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.~~

~~**Reference to prior version:** (Part 3.1) CIP-009, R1 and R3~~

~~**Change Description and Justification:** (Part 3.1)~~

~~Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.~~

~~**Reference to prior version:** (Part 3.2) New Requirement~~

~~**Change Description and Justification:** (Part 3.2)~~

~~Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.~~



**Version History**

Version	Date	Action	Change Tracking
<del>1</del>	<del>1/16/06</del>	<del>R3.2 — Change “Control Center” to “control center”</del>	<del>3/24/06</del>
<del>2</del>	<del>9/30/09</del>	<del>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. Reworking of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.</del>	
<del>3</del>		<del>Updated version number from <del>2</del> to <del>3</del> 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.</del>	
<del>3</del>	<del>12/16/09</del>	<del>Approved by the NERC Board of Trustees.</del>	<del>Update</del>
<del>3</del>	<del>3/31/10</del>	<del>Approved by FERC.</del>	
<del>4</del>	<del>12/30/10</del>	<del>Modified to add specific criteria for Critical Asset identification.</del>	<del>Update</del>
<del>4</del>	<del>1/24/11</del>	<del>Approved by the NERC Board of Trustees.</del>	
<del>5</del>	<del>11/26/12</del>	<del>Adopted by the NERC Board of Trustees.</del>	<del>Modified to coordinate with other CIP standards and to revise format to use RBS Template.</del>
<del>5</del>	<del>11/22/13</del>	<del>FERC Order issued approving CIP-009-5. (Order becomes effective on 2/3/14.)</del>	
<del>5</del>	<del>4/2/14</del>	<del>Address directive in FERC Order 791 to modify VSLs in Requirement R3</del>	<del>VSLs — R3</del>

**Reliability Standard CIP-010-2 Clean and Redline**

## A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments
2. **Number:** CIP-010-2
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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
    - 4.1.3 **Generator Operator**
    - 4.1.4 **Generator Owner**
    - 4.1.5 **Interchange Coordinator or Interchange Authority**

**4.1.6 Reliability Coordinator**

**4.1.7 Transmission Operator**

**4.1.8 Transmission Owner**

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

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-010-2:

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

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

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

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

**4.2.3.5** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. Effective Dates:**

See Implementation Plan for CIP-010-2.

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

**B. Requirements and Measures**

- R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 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-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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

CIP-010-2 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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<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"> <li>• 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</li> <li>• Documentation that the change was performed in accordance with the requirement.</li> </ul>



CIP-010-2 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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For a change that deviates from the existing baseline configuration:</p> <ol style="list-style-type: none"> <li>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;</li> <li>1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and</li> <li>1.4.3. Document the results of the verification.</li> </ol>	<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-010-2 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>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 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-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	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-010-2 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-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>At least once every 15 calendar months, conduct a paper or active vulnerability assessment.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• A document listing the date of the assessment and the output of any tools used to perform the assessment.</li> </ul>

CIP-010-2 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-010-2 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PCA</li> </ol>	<p>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.</p>	<p>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.</p>
3.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>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.</p>	<p>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).</p>

- 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:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Additional Compliance Information:

None



2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R1</b>	<b>Operations Planning</b>	<b>Medium</b>	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1)  OR  The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)  OR  The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)</p> <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</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>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 configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 &amp; 1.4.3)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<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>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R2</b>	<b>Operations Planning</b>	<b>Medium</b>	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
<b>R3</b>	<b>Long-term Planning and Operations Planning</b>	<b>Medium</b>	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>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>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>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>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</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
<b>R4</b>	<b>Long-term Planning and Operations Planning</b>	<b>Medium</b>	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and



R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>manage its Transient Cyber Asset(s) according to CIP-010-2, 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 according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for</p>	<p>implement the Removable Media sections according to CIP-010-2, 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 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</p>	<p>authorize its Transient Cyber Asset(s) according to CIP-010-2, 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 vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible</p>	<p>Removable Media according to CIP-010-2, Requirement R4. (R4)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)</p>	<p>CIP-010-2, 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-010-2, Requirement R4, Attachment 1,</p>	<p>Entity according to CIP-010-2, 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-010-2, Requirement</p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Sections 2.1, 2.2, and 2.3. (R4)	R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

Guideline and Technical Basis (attached).

**Version History**

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

## CIP-010-2 - Attachment 1

### Required Sections for Plans for Transient Cyber Assets and Removable Media

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

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

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

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

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

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

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

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

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

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

**Section 3.** Removable Media

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

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

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

## CIP-010-2 - Attachment 2

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

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

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

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

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

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



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

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

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

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

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

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

## Guidelines and Technical Basis

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

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

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

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

#### **Requirement R1:**

##### **Baseline Configuration**

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

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

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

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

### Asset #051028 at Substation Alpha

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

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

### **Cyber Security Controls**

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

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

### **Test Environment**

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

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

### **Requirement R2:**

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

### **Requirement R3:**

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

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

### Active Vulnerability Assessment:

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

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

### **Requirement R4:**

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

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

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;

- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

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

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

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

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

### Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

### Per Transient Cyber Asset Capability

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

types of devices, implementation of the antivirus software would not be required for those devices.

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

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

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

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

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

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



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

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

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

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update

of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

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

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.

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

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

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

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.<sup>1</sup> Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

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

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.

---

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

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

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

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

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

### **Requirement R4, Attachment 1, Section 3 - Removable Media**

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

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

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

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. 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:**

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

**Rationale for Requirement R1:**

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

**Rationale for Requirement R2:**

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

**Rationale for Requirement R3:**

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

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

**Rationale for R4:**

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

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

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

**Summary of Changes:** All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

## A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments
2. **Number:** CIP-010-~~12~~
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 ~~BES~~ Bulk Electric System (BES).
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~ SPS or ~~Remedial Action Scheme~~ 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

**4.2.1.2** Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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-~~12~~:

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

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



- 4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
- 4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. **Effective Dates:**

- ~~1. **24 Months Minimum** — CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~
- ~~2. — In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~See Implementation Plan for CIP-010-2.~~

6. **Background:**

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

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

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

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

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

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

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

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

**B. Requirements and Measures**

- R1.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in ~~CIP-010-12~~ 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-010-12~~ Table R1 – Configuration Change Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010- <del>12</del> 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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Develop a baseline configuration, individually or by group, which shall include the following items:</p> <ol style="list-style-type: none"> <li>1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;</li> <li>1.1.2. Any commercially available or open-source application software (including version) intentionally installed;</li> <li>1.1.3. Any custom software installed;</li> <li>1.1.4. Any logical network accessible ports; and</li> <li>1.1.5. Any security patches applied.</li> </ol>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or</li> <li>• A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.</li> </ul>

**CIP-010-~~42~~ 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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<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"> <li>• 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</li> <li>• Documentation that the change was performed in accordance with the requirement.</li> </ul>

**CIP-010-~~42~~ 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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>For a change that deviates from the existing baseline configuration:</p> <ol style="list-style-type: none"> <li>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;</li> <li>1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and</li> <li>1.4.3. Document the results of the verification.</li> </ol>	<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-~~42~~ 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>

- R2.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in CIP-010-~~12~~ 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-~~12~~ Table R2 – Configuration Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010- <del>12</del> Table R2 – Configuration Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol>	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 ~~processes~~process(es) that collectively include each of the applicable requirement parts in CIP-010-~~12~~ 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-~~12~~ Table R3 – Vulnerability Assessments and additional evidence to demonstrate implementation as described in the Measures column of the table.



CIP-010- <del>12</del> 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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>At least once every 15 calendar months, conduct a paper or active vulnerability assessment.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• 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<del>72</del> or</li> <li>• A document listing the date of the assessment and the output of any tools used to perform the assessment.</li> </ul>

**CIP-010-~~12~~ 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-~~12~~ 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"> <li>1. EACMS;</li> <li>2. PCA</li> </ol>	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"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

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

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1 Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority (~~“(“ (CEA”) unless~~) means NERC or the applicable entity is owned, operated, or controlled by Regional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEANERC Reliability Standards.

#### 1.2 Evidence Retention:

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

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

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

#### 1.3 Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

~~Complaint~~Complaints

#### 1.4 Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	<p>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)</p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline</del></p>	<p>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> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies</del></p>	<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><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline</del></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><del>The Responsible Entity has documented and</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p>	<p><del>but did not assess and correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be</del></p>	<p><del>items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p>	<p><del>implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify,</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)</p> <p>OR</p> <p>The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify,</p>	<p>impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (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 configuration but did not identify, assess, or correct the deficiencies in the</p>	<p>The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)</p> <p>OR</p> <p>The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify,</p>	<p><del>assess, and correct the deficiencies. (1.1)</del></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> <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>



R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><del>assess, or correct the deficiencies in the verification documentation. (1.4.3)</del></p>	<p><del>determination of affected security controls. (1.4.1)</del></p>	<p><del>assess, or correct the deficiencies. (1.2)</del></p> <p>OR</p> <p><del>The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3)</del></p> <p>OR</p> <p><del>The Responsible Entity has a process(es) to update baseline configurations</del></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 configuration but did</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess,</del></p>	<p>not verify and document that the required controls were not adversely affected following the change. (1.4.2 &amp; 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,</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>or correct the deficiencies. (1.4.2)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process for testing changes in an environment that models the</del></p>	document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct</del></p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>the deficiencies. (1.5.1)</del></p> <p>OR</p> <p><del>The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the deficiencies. (1.5.2)</del></p> <p>OR</p> <p><del>The Responsible Entity has a process to document the test results and, if using a test environment,</del></p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p><del>document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)</del></p>	
R2	Operations Planning	Medium	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. <del>(2.1)</del></p> <p><del>OR</del></p> <p><del>The Responsible Entity has documented and implemented a</del></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p><del>process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1)</del></p> <p>OR</p> <p>The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess,</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<del>or correct the deficiencies. (2.1)(2.1)</del>
<b>R3</b>	<b>Long-term Planning and Operations Planning</b>	<b>Medium</b>	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3)  OR The Responsible Entity has implemented one or more documented



R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>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>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>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>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</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
<b><u>R4</u></b>	<b><u>Long-term Planning and Operations Planning</u></b>	<b><u>Medium</u></b>	<b><u>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to</u></b>	<b><u>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to</u></b>	<b><u>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to</u></b>	<b><u>The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and</u></b>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><u>manage its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.1. (R4)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity documented its plan(s) for</u></p>	<p><u>implement the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to</u></p>	<p><u>authorize its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible</u></p>	<p><u>Removable Media according to CIP-010-2, Requirement R4. (R4)</u></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p><u>Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)</u></p>	<p><u>CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)</u></p> <p>OR</p> <p><u>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-010-2, Requirement R4, Attachment 1,</u></p>	<p><u>Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)</u></p> <p>OR</p> <p><u>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-010-2, Requirement</u></p>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>Sections 2.1, 2.2, and 2.3. (R4)</u>	<u>R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)</u>	

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

~~None.~~

Guideline and Technical Basis (attached).

**Version History**

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>1</u>	<u>11/26/12</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>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.</u>
<u>1</u>	<u>11/22/13</u>	<u>FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)</u>	
<u>2</u>	<u>11/13/14</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.</u>
<u>2</u>	<u>2/12/15</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>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.</u>

## CIP-010-2 - Attachment 1

### Required Sections for Plans for Transient Cyber Assets and Removable Media

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

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

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



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

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

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

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

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

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

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

**Section 3. Removable Media**

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

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

**3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:**

**3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and**

**3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.**

## CIP-010-2 - Attachment 2

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

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

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

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

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

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

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

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

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

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

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

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

## Guidelines and Technical Basis

### 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-~~5.1~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

#### **Requirement R1:**

##### **Baseline Configuration**

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

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

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-56. 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-007-56 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

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

### Asset #051028 at Substation Alpha

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

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

## **Cyber Security Controls**

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

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

### **Test Environment**

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

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

### **Requirement R2:**

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

### **Requirement R3:**

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

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.



## Guidelines and Technical Basis

---

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

### Active Vulnerability Assessment:

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

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

### Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

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

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;

- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

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

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

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

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

### Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

### Per Transient Cyber Asset Capability

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

types of devices, implementation of the antivirus software would not be required for those devices.

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

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

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

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

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

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

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

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

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

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update

of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

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

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.

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

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

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

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.<sup>1</sup> Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

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

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.

---

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

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

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

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

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

### **Requirement R4, Attachment 1, Section 3 - Removable Media**

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

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

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

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. 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:**

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts text boxes~~ were embedded within the standard ~~to explain the rationale for various parts of the standard~~. Upon BOT approval, ~~that information~~ the text from the rationale text boxes was moved to this section.

**Rationale for Requirement R1:**

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

~~Reference to prior version: (Part 1.1) New Requirement~~

~~Change Rationale: (Part 1.1)~~

~~The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.~~

~~Reference to prior version: (Part 1.2) CIP-007-3, R9; CIP-003-3, R6~~

~~Change Rationale: (Part 1.2)~~

~~The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.~~

~~Reference to prior version: (Part 1.3) CIP-007-3, R9; CIP-005-3, R5~~

~~Change Rationale: (Part 1.3)~~

~~Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.~~

~~Reference to prior version: (Part 1.4) CIP-007-3, R1~~

~~Change Rationale: (Part 1.4)~~

~~The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.~~

~~Reference to prior version: (Part 1.5) CIP-007-3, R1~~

~~Change Rationale: (Part 1.5)~~

~~This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.~~

~~This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.~~

**Rationale for Requirement R2:**

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

~~Reference to prior version: (Part 2.1) New Requirement~~

~~Change Rationale: (Part 2.1)~~

~~The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.~~

~~This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.~~

~~Thirty five Calendar days allows for a “once-a-month” frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.~~

**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.

~~Reference to prior version: (Part 3.1) CIP-005-4, R4; CIP-007-4, R8~~

~~Change Rationale: (Part 3.1)~~

~~As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.~~

~~Reference to prior version: (Part 3.2) New Requirement~~

~~Change Rationale: (Part 3.2)~~

~~FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.~~

~~As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.~~

~~Reference to prior version: (Part 3.3) New Requirement~~

~~Change Rationale: (Part 3.3)~~

~~FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.~~

~~Reference to prior version: (Part 3.4) CIP-005-3, R4.5; CIP-007-3, R8.4~~

~~Change Rationale: (Part 3.4)~~

~~Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.~~

### Version History

Version	Date	Action	Change Tracking
---------	------	--------	-----------------

## Guidelines and Technical Basis

†	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.
†	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	

### **Rationale for Requirement R4:**

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

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

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

**Summary of Changes:** All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

**Reliability Standard CIP-011-2 Clean and Redline**

## A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-2
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
    - 4.1.3 **Generator Operator**
    - 4.1.4 **Generator Owner**
    - 4.1.5 **Interchange Coordinator or Interchange Authority**
    - 4.1.6 **Reliability Coordinator**

**4.1.7 Transmission Operator**

**4.1.8 Transmission Owner**

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

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-011-2:

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

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

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

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

**4.2.3.5** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. Effective Dates:**

See Implementation Plan for CIP-011-2.

**6. Background:**

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

**“Applicable Systems” Columns in Tables:**

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

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



## B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].
- M1.** Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R1 – Information Protection			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Method(s) to identify information that meets the definition of BES Cyber System Information.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Documented method to identify BES Cyber System Information from entity’s information protection program; or</li> <li>• Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity’s information protection program; or</li> <li>• Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or</li> <li>• Repository or electronic and physical location designated for housing BES Cyber System Information in the entity’s information protection program.</li> </ul>

CIP-011-2 Table R1 – Information Protection			
Part	Applicable Systems	Requirement	Measure
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or</li> <li>• Records indicating that BES Cyber System Information is handled in a manner consistent with the entity’s documented procedure(s).</li> </ul>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or</li> <li>• Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.</li> </ul>

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or</li> <li>• Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.</li> </ul>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

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

#### 1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	Operations Planning	Lower	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

Guideline and Technical Basis (attached).

**Version History**

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.



## Guidelines and Technical Basis

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

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

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

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

#### **Requirement R1:**

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity’s information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity’s BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

### **Requirement R2:**

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

**Clear:** One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].

**Purge:** Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

**Destroy:** There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

### **Rationale:**

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

#### **Rationale for Requirement R1:**

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

#### **Rationale for Requirement R2:**

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

## A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-~~12~~
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the ~~BES~~. Bulk Electric System (BES).
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

**4.2.1.1** Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

**4.2.3 Exemptions:** The following are exempt from Standard CIP-011-~~12~~:

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

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

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

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

**4.2.3.5** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. Effective Dates:**

~~1. **24 Months Minimum**—CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees’ approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-011-2.

**6. Background:**

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

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

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

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any

particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the "... identifies, assesses, and corrects deficiencies, ..." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

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

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

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

Measures 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~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

**"Applicable Systems" Columns in Tables:**



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

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

## B. Requirements and Measures

- R1.** Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~12~~ Table R1 – Information Protection*. [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].
- M1.** Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~12~~ Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~12~~ Table R1 – Information Protection

Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Method(s) to identify information that meets the definition of BES Cyber System Information.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Documented method to identify BES Cyber System Information from entity’s information protection program; or</li> <li>• Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity’s information protection program; or</li> <li>• Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or</li> <li>• Repository or electronic and physical location designated for housing BES Cyber System Information in the entity’s information protection program.</li> </ul>

CIP-011- <del>12</del> Table R1 – Information Protection			
Part	Applicable Systems	Requirement	Measure
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PACS</li> </ol>	<p>Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or</li> <li>• Records indicating that BES Cyber System Information is handled in a manner consistent with the entity’s documented procedure(s).</li> </ul>

- R2.** Each Responsible Entity shall implement one or more documented ~~processes~~process(es) that collectively include the applicable requirement parts in CIP-011-~~12~~ Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-011-~~12~~ Table R2 – BES Cyber Asset Reuse and Disposal and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011- <del>12</del> Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or</li> <li>• Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.</li> </ul>

CIP-011-~~12~~ Table R2 – BES Cyber Asset Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol> <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS;</li> <li>2. PACS; and</li> <li>3. PCA</li> </ol>	<p>Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or</li> <li>• Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.</li> </ul>

## C. Compliance

### 1. Compliance Monitoring Process:

#### 1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority (~~“(“ (CEA”) unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. ~~In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

#### 1.2. Evidence Retention:

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

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

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

#### 1.3. Compliance Monitoring and Assessment Processes:

- Compliance ~~Audit~~Audits
- Self-~~Certification~~Certifications
- Spot Checking
- Compliance ~~Investigation~~Violation Investigations
- Self-Reporting
- ~~Complaint~~
- Complaints

#### 1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	<u>N/A</u>	<p><del>The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies.-(1.1)</del></p> <p>OR</p> <p><del>The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify,</del></p>	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).



R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<del>assess, or correct the deficiencies. (1.1)</del> OR <del>The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2)</del> OR <del>The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information</del>	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- <del>12</del> )			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<del>but did not identify, assess, or correct the deficiencies. (1.2)</del> <u>N/A</u>	
<b>R2</b>	<b>Operations Planning</b>	<b>Lower</b>	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011- <del>12</del> Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

~~None.~~

Guideline and Technical Basis (attached).

**Version History**

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
<u>1</u>	<u>11/26/12</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.</u>
<u>1</u>	<u>11/22/13</u>	<u>FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)</u>	
<u>2</u>	<u>11/13/14</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.</u>
<u>2</u>	<u>2/12/15</u>	<u>Adopted by the NERC Board of Trustees.</u>	<u>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.</u>

## 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-~~5.1~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

#### Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity’s information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity’s BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. [This includes information that may be stored on Transient Cyber Assets or Removable Media.](#)

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

### **Requirement R2:**

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the ~~responsible entity~~ Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

**Clear:** One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].

**Purge:** Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

#### Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts text boxes~~ were embedded within the standard ~~to explain the rationale for various parts of the standard~~. Upon BOT approval, ~~that information~~ the text from the rationale text boxes was moved to this section.

#### Rationale for **Requirement R1**:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

~~**Summary of Changes:** CIP-003-4 R4, R4.2, and R 4.3 have been moved to CIP-011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.~~

~~**Reference to prior version:** (Part 1.1) CIP-003-3, R4; CIP-003-3, R4.2~~

~~**Change Rationale:** (Part 1.1)~~

~~The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (e.g., confidential, public, internal use only, etc.) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.~~

~~**Reference to prior version:** (Part 1.2) CIP-003-3, R4~~

~~**Change Rationale:** (Part 1.2)~~

~~The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.~~

**Rationale for Requirement R2:**

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

~~**Reference to prior version:** (Part 2.1) CIP-007-3, R7.2~~

~~**Change Rationale:** (Part 2.1)~~

~~*Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal.*~~

~~**Reference to prior version:** (Part 2.2) CIP-007-3, R7.1~~

~~**Change Rationale:** (Part 2.2)~~

~~*Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal.*~~

~~*The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*~~



## Version History

Version	Date	Action	Change Tracking
<del>1</del>	<del>11/26/12</del>	<del>Adopted by the NERC Board of Trustees.</del>	<del>Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.</del>
<del>1</del>	<del>11/22/13</del>	<del>FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)</del>	

## **Definition of Terms Used in Standards**

## Definitions of Terms Used in Standards

*This section includes new and modified defined terms used in the proposed standards. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New definitions listed below become approved when the proposed standards are approved. When the standards become effective, these defined terms will be added to the Glossary.*

**BES Cyber Asset (BCA):** A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

**Low Impact BES Cyber System Electronic Access Point (LEAP):** A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

**Low Impact External Routable Connectivity (LERC):** Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

**Protected Cyber Assets (PCA):** One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

**Removable Media:** Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

**Transient Cyber Asset:** A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to,

Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

## Definitions of Terms Used in Standards

*This section includes revised terms used in the proposed standards. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. Revised definitions listed below become approved when the proposed standards are approved. When the standards become effective, these defined terms will be added to the Glossary.*

### Redline to Last Approved

**BES Cyber Asset (BCA):** A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. ~~(A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)~~

**Protected Cyber Assets (PCA):** One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. ~~A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.~~