

## Standard Development Timeline

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

### Description of Current Draft

This is the initial draft of proposed standard.

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

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

## A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems
2. **Number:** CIP-006-7
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 (BCS) against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
  - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
    - 4.1.1 **Balancing Authority**
    - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
      - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
        - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
        - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
      - 4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
      - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
    - 4.1.3 **Generator Operator**

- 4.1.4 Generator Owner
- 4.1.5 Reliability Coordinator
- 4.1.6 Transmission Operator
- 4.1.7 Transmission Owner

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

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

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

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

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

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

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

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

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

**4.2.3 Exemptions:** The following are exempt from Standard CIP-006-7:

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

**4.2.3.2** Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

- 4.2.3.3 Cyber Systems, associated with communication links, between CyberSystems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.
- 4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
- 4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**4.3. “Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

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

## 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-006-7 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-006-7 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-006-7 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact BCS without External Routable Connectivity (ERC) SCI without ERC hosting Medium Impact BCS Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> <li>• High Impact BCS</li> <li>• Medium Impact BCS with ERC</li> </ul> SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.2 or Part 1.3	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-006-7 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.2	<p>Medium Impact BCS with ERC and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.3</p>	<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>
1.3	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI identified independently supporting an Applicable System above</p>	<p>Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.</p>	<p>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.</p>

CIP-006-7 Table R1— Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BCS with ERC and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI identified independently supporting an Applicable System above</p>	<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>
1.5	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BCS with ERC and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI identified independently supporting an Applicable System above</p>	<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 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>

CIP-006-7 Table R1— Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.6	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> <li>• High Impact BCS, or</li> </ul> Medium Impact BCS with ERC SCI identified independently supporting an Applicable System above	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> <li>• High Impact BCS, or</li> <li>• Medium Impact BCS with ERC</li> </ul> SCI identified independently supporting an Applicable System above	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the 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-006-7 Table R1— Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.8	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BCS with ERC and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI identified independently supporting an Applicable System above</p>	<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, except during CIP Exceptional Circumstances.</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>
1.9	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BCS with ERC and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI identified independently supporting an Applicable System above</p>	<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, except during CIP Exceptional Circumstances.</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>

- R2.** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 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-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BCS and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> Medium Impact BCS with ERC and their associated: <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> SCI identified independently supporting an Applicable System above	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter.	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.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.2.	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BCS with EERC and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI identified independently supporting an Applicable System above</p>	<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 BCS and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>Medium Impact BCS with ERC and their associated:</p> <ol style="list-style-type: none"> <li>1. EACMS; and</li> <li>2. PCA</li> </ol> <p>SCI identified independently supporting an Applicable System above</p>	<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-006-7 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-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 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 BCS</li> <li>• Medium Impact BCS with ERC</li> <li>• SCI identified independently supporting a High Impact BCS; or</li> <li>• SCI identified independently supporting a Medium Impact BCS with ERC</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 BCS</li> <li>• Medium Impact BCS with ERC</li> <li>• SCI identified independently supporting a High Impact BCS; or</li> <li>• SCI identified independently supporting a Medium Impact BCS with ERC</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 Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

## Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	<p>The Responsible Entity did not document or implement physical security plans. (Requirement R1)</p> <p>OR</p> <p>The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Requirement R1 Part 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. (Requirement R1 Part 1.2)</p> <p>OR</p> <p>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. (Requirement R1 Part 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</p>

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>Physical Security Perimeter. (Requirement R1 Part 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. (Requirement R1 Part 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. (Requirement R1 Part 1.6)</p> <p>OR</p> <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. (Requirement R1 Part 1.7)</p> <p>OR</p> <p>The Responsible Entity does not have a process to log authorized physical entry into</p>

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9)
R2	N/A	N/A	N/A	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. (Requirement R2 Part 2.1) OR 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. (Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)



R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
<b>R3</b>	<p>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 24 calendar months but did complete required testing within 25 calendar months. (Requirement R3 Part 3.1)</p>	<p>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. (Requirement R3 Part 3.1)</p>	<p>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. (Requirement R3 Part 3.1)</p>	<p>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. (Requirement R3 Part 3.1)</p> <p>OR</p> <p>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. (Requirement R3 Part 3.1)</p>

**D. Regional Variances**

None.

**E. Interpretations**

None.

**F. Associated Documents**

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

## Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	<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

Version	Date	Action	Change Tracking
			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.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes and CEC language added	