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 networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

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

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

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

4.3. **"Applicable Systems":** 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 Modifications 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) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP 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.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 　1. EACMS; and 　2. PCA SCI supporting an Applicable System in this Part	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP 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.
1.4	High impact BCS and their associated: 　1. EACMS; and 　2. PCA Medium impact BCS with ERC and their associated: 　1. EACMS; and 　2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High impact BCS and their associated: 　1. EACMS; and 　2. PCA Medium impact BCS with ERC and their associated: 　1. EACMS; and 　2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are 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 PSP and additional evidence that the alarm or alert was issued and communicated as identified in the 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.
1.6	Physical Access Control Systems (PACS) associated with: 　• High impact BCS, or 　• Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Monitor each PACS for unauthorized physical access to a PACS.	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	PACS associated with: 　• High impact BCS, or 　• Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are 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 PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the 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	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP.
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

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: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from each PSP 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.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures

2.3	High impact BCS and their associated:
	    1. EACMS; and
	    2. PCA
	
	 Medium impact BCS with ERC and their associated:
	    1. EACMS; and
	    2. PCA
	
	 SCI supporting an Applicable System in this Part
		Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

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	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: • High impact BCS, or • Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable each PSP 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:** 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:** 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	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 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. (Part 1.3) OR The Responsible Entity does not have a process to monitor

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				for unauthorized access through a physical access point into a PSP. (Part 1.4)
				OR
				The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5)
				OR
				The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6)
				OR
				The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7)
				OR
				The Responsible Entity does not have a process to log

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				authorized physical entry into each PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (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. (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. (Part 2.2) OR The Responsible Entity failed to include or implement a

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				visitor control program to retain visitor logs for at least 90 days. (Part 2.3)
R3	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. (Part 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 PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for PACS 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. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02

- CIP-006-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
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	5/9/2024	Adopted by the NERC Board of Trustees.	Virtualization Modifications by Project 2016-02