## A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7~~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 in this standard~~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 explicitly 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~~4.1.5~~** **Reliability Coordinator**

**4.1.7~~4.1.6~~** **Transmission Operator**

**4.1.8~~4.1.7~~** **Transmission Owner**

**4.2.** **Facilities:** For the ~~purpose of the~~ requirements in this standard~~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 explicitly 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~~CIP-006-7:

**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 BES Cyber Systems' Logical Isolation Zones. ~~discrete Electronic Security Perimeters~~.

**4.2.3.3** Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

**~~4.2.3.2~~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.

**~~4.2.3.3~~4.2.3.5**   For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

**~~4.2.3.4~~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-002-5.1 identification and categorization processes.

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

See Implementation Plan for CIP-006-7~~6~~.

## 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-006-76 Table R1 – Physical Security Plan*.

**M1.**    Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-76 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-006-76 Table R1 –   Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | Medium Impact BES Cyber Systems without External Routable Connectivity<br><br>Physical Access Control Systems (PACS) associated with:<br><br>• High Impact BES Cyber Systems, or<br><br>• Medium Impact BES Cyber Systems with External Routable Connectivity | 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-006-76 Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.2 | Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br><br>   1.  EACMS; and<br><br>   2.  PCSA | Usetilize 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. | 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. |

| CIP-006-76 Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| Part | Applicable Systems | Requirements | Measures |
| 1.3 | High Impact BES Cyber Systems and their associated:<br><br>1. EACMS; and<br><br>2. PCSA | Where technically feasible, use~~tilize~~ 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-006-76 Table R1– Physical Security Plan | | | |
|------|------|------|------|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.4 | High Impact BES Cyber Systems and their associated:<br><br>1. EACMS; and<br><br>2. PCSA<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br><br>1. EACMS; and<br><br>2. PCSA | Monitor for unauthorized access through a physical access point into a Physical Security Perimeter. | 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. |

| CIP-006-76 Table R1–   Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.5 | High Impact BES Cyber Systems and their associated:<br><br>1. EACMS; and<br><br>2. PCSA<br><br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br><br>1. EACMS; and<br><br>2. PCSA | 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. | 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. |
| 1.6 | Physical Access Control Systems (PACS) associated with:<br><br>• High Impact BES Cyber Systems, or<br><br>• Medium Impact BES Cyber Systems with External Routable Connectivity | 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. |

| CIP-006-76 Table R1– Physical Security Plan | | | |
|------|------|------|------|
| Part | Applicable Systems | Requirements | Measures |
| 1.7 | Physical Access Control Systems (PACS) associated with:<br><br>• High Impact BES Cyber Systems, or<br><br>• Medium Impact BES Cyber Systems with External Routable Connectivity | 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-006-7̶6̶ Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| Part | Applicable Systems | Requirements | Measures |
| 1.8 | High Impact BES Cyber Systems and their associated:<br><br>1. EACM̶S; and<br><br>2. PCS̶A̶<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br><br>1. EACM̶S; and<br><br>2. PCS̶A̶ | 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. | 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. |

| CIP-006-76 Table R1 – Physical Security Plan |||| 
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.9 | High Impact BES Cyber Systems and their associated:<br><br>1. EACMS; and<br><br>2. PCSA<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br><br>1. EACMS; and<br><br>2. PCSA | 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. | 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. |

| CIP-006-6CIP-006-7 Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.10 | High Impact BES Cyber Systems and their associated PCS~~A~~

Medium Impact BES Cyber Systems at Control Centers and their associated ~~:~~

PCS~~A~~ | Restrict physical access to cabling and other nonprogrammable communication components used for ~~connection between~~ applicable ~~Cyber Assets~~systems ~~within~~ in the same ~~Electronic Security~~Logical Isolation Zone ~~Perimeter~~ in those instances when such cabling and components are located outside of a Physical Security Perimeter.

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:

• encryption of data that transits such cabling and components; or

• 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

• an equally effective logical protection. | 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. |

**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-006-76 Table R2 – Visitor Control Program.*

**M2.** Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-76 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-006-76 Table R2 – Visitor Control Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact BES Cyber Systems and their associated: <br> 1. EACMS; and <br> 2. PCSA <br><br> Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <br> 1. EACMS; and <br> 2. PCSA | 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. | 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 escorted access process was implemented, such as visitor logs. |

| CIP-006-76 Table R2 – Visitor Control Program | | | |
|------|------|------|------|
| Part | Applicable Systems | Requirements | Measures |
| 2.2 | High Impact BES Cyber Systems and their associated:<br><br>   1. EACMS; and<br>   2. PCSA<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br><br>   1. EACMS; and<br>   2. PCSA | 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. | 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 escorted access process was implemented, such as dated visitor logs that include the required information. |
| 2.3 | High Impact BES Cyber Systems and their associated:<br><br>   1. EACMS; and<br>   2. PCSA<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br><br>   1. EACMS; and<br>   2. PCSA | Retain visitor logs for at least ninety calendar days. | An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety 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~~6 Table R3 – Maintenance and Testing Program*.

**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~~6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-006-~~7~~6 Table R3 – Physical Access Control System Maintenance and Testing Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirement** | **Measures** |
| 3.1 | Physical Access Control Systems (PACS) associated with:<br><br>• High Impact BES Cyber Systems, or<br><br>• Medium Impact BES Cyber Systems with External Routable Connectivity<br><br>Locally mounted hardware or devices at the Physical Security Perimeter associated with:<br><br>• High Impact BES Cyber Systems, or<br><br>• Medium Impact BES Cyber Systems with External Routable Connectivity | 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, Also, ~~and~~ additional evidence such as dated maintenance records or other documentation ~~to demonstrate that this testing was done, such as dated maintenance records, or other documentation~~ to demonstrate that ~~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:**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

**1.4. Additional Compliance Information:**

None

## 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. |
| 6 | 1/21/16 | FERC order issued approving CIP-006-6. Docket No. RM15-14-000 | |