Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

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	

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version	Date	Action	Change Tracking
		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	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

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

2. **Number:** CIP-006-5

3. **Purpose:** Standard CIP-006-5 requires the implementation of a physical security plan for the protection of 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 Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 **Interchange Coordinator**

4.1.6 **Load-Serving Entity** that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 **NERC**

4.1.8 **Regional Entity**

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-006-5

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

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

4.2.4.3 In nuclear plants, 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.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 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*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

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 specific elements required. in the documented processes.. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

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 infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel 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.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the 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.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. 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.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 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.
- **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 identification and categorization processes.
- **Low Impact BES Cyber Systems** – Applies to BES Cyber Systems not categorized as High Impact or Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These

hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 were intended to constitute a physical security program, though there was no specific requirement dictating the need for such a program, only physical security plans.

Added details to address FERC Order 706, paragraph 572 directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address FERC Order 706 p575 directive.

R1. Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*

M1. Evidence must includes each of the documented physical security plan or plans that collectively include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Associated Physical Access Control Systems Low Impact BES Cyber Systems.	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c R2.1 for Physical Access Control Systems* *New Requirement for Low Impact BES Cyber Systems*		**Change Description and Justification:** *To allow for programmatic protection controls as a baseline, this includes how the entity plans to protect Low Impact BES Cyber Systems and does not require detailed list of individuals with access.*	

<table>
<tr><th colspan="4">CIP-006-5 Table R1 – Physical Security Plan</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>1.2</td><td>Medium Impact BES Cyber Systems.
Associated Electronic Access Control or Monitoring Systems
Associated Protected Cyber Assets</td><td>Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.</td><td>Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
<i>CIP006-4c R3 &amp; R4</i></td><td colspan="2"><b>Change Description and Justification:</b> <i>This requirement has been made more general to allow for alternate measures of restricting physical access to reflect the change from Physical Security Perimeter to Defined Physical Boundary. 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 .</i></td></tr>
</table>

<table>
<tr><th colspan="4">CIP-006-5 Table R1 – Physical Security Plan</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>1.3</td><td>High Impact BES Cyber Systems
Associated Electronic Access Control or Monitoring Systems
Associated Protected Cyber Assets</td><td>Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.</td><td>Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
CIP006-4c R3 & R4</td><td colspan="2"><b>Change Description and Justification:</b> <i>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.</i>
<i>Added to address FERC Order 706 p572 related directives for physical security defense in depth.</i>
<i>FERC Order 706 p575 directives addressed by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered defined physical boundary(s).</i></td></tr>
</table>

<table>
<tr><th colspan="4">CIP-006-5 Table R1 – Physical Security Plan</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>1.4</td><td>High Impact BES Cyber Systems
Medium Impact BES Cyber Systems
Associated Electronic Access Control or Monitoring Systems
Associated Protected Cyber Assets</td><td>Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.</td><td>Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
<i>CIP006-4c R5</i></td><td colspan="2"><b>Change Description and Justification:</b> <i>Examples of monitoring methods have been moved to the Guidelines and Technical Basis section..</i></td></tr>
<tr><td>1.5</td><td>Associated Physical Access Control Systems</td><td>Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.</td><td>Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b> CIP006-4c R2.2</td><td colspan="2"><b>Change Description and Justification:</b> <i>Addresses the old CIP-006-4c R5 requirement for Physical Access Control Systems.</i></td></tr>
</table>

<table>
<tr><th colspan="4">CIP-006-5 Table R1 – Physical Security Plan</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>1.6</td><td>High Impact BES Cyber Systems
Medium Impact BES Cyber Systems
Associated Electronic Access Control or Monitoring Systems
Associated Protected Cyber Assets</td><td>Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.</td><td>Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into Defined Physical Boundaries and additional evidence to demonstrate that this logging and recording has been implemented, such as logs of physical access into Defined Physical Boundaries that show the date of entry into Defined Physical Boundaries.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b> CIP-006-4c R6</td><td colspan="2"><b>Change Description and Justification:</b> <i>CIP-006-4c R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the</i> Defined Physical Boundary.
<i>Examples of logging methods have been moved to the Guidelines and Technical Basis section .</i></td></tr>
</table>

Rationale: To control when personnel without authorized unescorted physical access can be in any Defined Physical Boundaries protecting BES Cyber Systems or Electronic Access Control 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.

R2. Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M2. Evidence must include the documented visitor control program that collectively includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Defined Physical Boundaries and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c R1.6.2*		**Change Description and Justification:** *No change.*	

<table>
<tr><th colspan="4">CIP-006-5 Table R2 – Visitor Control Program</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>2.2</td><td>High Impact BES Cyber Systems
Medium Impact BES Cyber Systems.
Associated Electronic Access Control or Monitoring Systems
Associated Protected Cyber Assets</td><td>A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor’s name, and individual point of contact.</td><td>Evidence may include, but is not limited to, a visitor control program that provides logging of the entry and exit of visitors including date, time, and visitor name along with the individual point of contact; dated visitor logs for each Defined Physical Boundary that include the same required information.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
<i>CIP-006-4c R1.6.1</i></td><td colspan="2"><b>Change Description and Justification:</b> <i>Addressed multi entry requirements and added the point of contact which is the person who can be considered the sponsor for the visitor. There is no need to document the escort or handoffs between escorts.</i></td></tr>
</table>

Rationale: 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 706, paragraph 581 directives for test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M3. Evidence must include each of the documented maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

<table>
<tr><th colspan="4">CIP-006-5 Table R3 – Maintenance and Testing Program</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirement</th><th>Measures</th></tr>
<tr><td>3.1</td><td>Associated Physical Access Control Systems
Locally mounted hardware or devices associated with Defined Physical Boundaries</td><td>Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.</td><td>Evidence may include, but is not limited to a maintenance and testing program that provides for testing the Physical Access Control Systems and locally mounted hardware or devices associated with Defined Physical Boundaries prior to commissioning and at least once every 24 calendar months thereafter, and provides additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed at least once on each applicable device or system at least once every 24 calendar months.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
<i>CIP-006-4c R8.1</i></td><td colspan="2"><b>Change Description and Justification:</b> <i>Added details to address FERC Order 706 p581 directives to test more frequently than every three years. It was felt annually testing was too often.</i></td></tr>
<tr><td>3.2</td><td>Associated Physical Access Control or Monitoring Systems</td><td>Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.</td><td>Evidence may include, but is not limited to, availability of the outage records.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
<i>CIP-006-4c R8.3</i></td><td colspan="2"><b>Change Description and Justification:</b> <i>Outage records shall be generated but the retention period is addressed in the retention section.</i></td></tr>
</table>

C. Compliance

1. Compliance Monitoring Process

5.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For responsible entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

5.2. 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 Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

5.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

5.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Defined Physical Boundary does not provide sufficient information to uniquely identify the individual and date of entry. (Part 1.7)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems (Part 1.5)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized access through any access point in a Defined Physical Boundary. (Part 1.4) OR The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. (Part 1.6)	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. OR The Responsible Entity has documented and implemented physical access controls, but two or more different and complementary methods do not exist to restrict access to High Impact BES Cyber Systems. (Part 1.3)
R2	**Same-Day**	**Medium**	N/A	The Responsible Entity included a visitor control program in its	The Responsible Entity included a visitor control program in its	The Responsible Entity has failed to include or implement a visitor

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations			physical security plan, but did not log each of the entry and exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact.	physical security plan, but it does not meet the requirements of continuous escort.	control program to provide required escorted access of visitors within any Defined Physical Boundary protecting BES Cyber Systems.
R3	**Long Term Planning**	**Lower**	N/A	The Responsible Entity has documented and implemented a maintenance and testing program, but the testing is not performed on a cycle of not more than 24 months.	The Responsible Entity has documented and implemented a maintenance and testing program, but not all outage records regarding access controls, logging, and alerting are generated as required.	The Responsible Entity has not documented and implemented maintenance and testing programs.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access 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 Defined Physical Boundary.

Methods to alert on 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 immediate notification to personnel 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 706 p572 directive, directed the intent of utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Defined Physical Boundaries, 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 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 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 (i.e. key or card key) would provide access through both.

Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.

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 Defined Physical Boundary 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.

It is also felt 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 Defined Physical Boundary. 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.

Outage records should address when the installed control, monitor and logging systems or hardware at access points are broken or unavailable.