Standard Development Roadmap

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. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1.Conduct initial ballot	April 2 - 11, 2009
2.Post response to comments on first ballot	April 20 - May 12, 2009
3.Conduct recirculation ballot	May 13 - 22, 2009
4.Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets

2. **Number:** CIP-006-~~2~~3

3. **Purpose:** Standard CIP-006-~~2~~3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. **Applicability:**

   4.1. Within the text of Standard CIP-006-~~2~~3, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator~~.~~

   4.1.2 Balancing Authority~~.~~

   4.1.3 Interchange Authority~~.~~

   4.1.4 Transmission Service Provider~~.~~

   4.1.5 Transmission Owner~~.~~

   4.1.6 Transmission Operator~~.~~

   4.1.7 Generator Owner~~.~~

   4.1.8 Generator Operator~~.~~

   4.1.9 Load Serving Entity~~.~~

   4.1.10 NERC~~.~~

   4.1.11 Regional Entity~~.~~

   4.2. The following are exempt from Standard CIP-006-~~2~~3:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-~~2~~3, identify that they have no Critical Cyber Assets~~.~~

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter ~~of personnel not authorized for unescorted access.~~.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3 Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- 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 to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures

specified in Requirement CIP-008-~~2.~~3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate 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 authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring 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 as specified in Requirement R4.

R7. Access Log Retention — The ~~responsible entity~~Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-~~2~~3 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	