A. Introduction

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

2. Number: CIP-006-1a

3. Purpose: Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-006, "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 Reliability Organizations.

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

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, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

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

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also 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 the Critical Cyber Assets.

R1.2. Processes to identify all 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. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days 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. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

R2. 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:

R2.1. 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.

R2.2. 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.

R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R3. 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. One or more of the following monitoring methods shall be used:

R3.1. 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.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

R4. 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:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. 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 R2.3.

R5. Access Log Retention — The 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.

R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:

R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.

R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

The physical security plan as specified in Requirement R1 and documentation of the review and updating of the plan.

Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.

Documentation identifying the methods for monitoring physical access as specified in Requirement R3.

Documentation identifying the methods for logging physical access as specified in Requirement R4.

Access logs as specified in Requirement R5.

Documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documents other than those specified in Requirements R5 and R6.2 from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

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

1.4.4 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 for that single access point at the dial-up device.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,

2.1.2 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.1.3 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

2.1.4 Physical access logs are retained for a period shorter than ninety days; or,

2.1.5 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

2.1.6 One required document does not exist.

2.2. Level 2:

2.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

2.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

2.2.4 More than one required document does not exist.

2.3. Level 3:

2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,

2.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

2.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.4.3 No maintenance or testing program exists.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 – Interpretation of Requirement R1.1 and additional Compliance Information Section 1.4.4 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Approved by Board of Trustees	New
1a	February 12, 2008	Added Appendix 1: Interpretation of R1 and Additional Compliance Information Section 1.4.4	Addition

Appendix 1

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

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

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also 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 the Critical Cyber Assets.

CIP-006-1 – Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 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 for that single access point at the dial-up device.