

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-4
3. **Purpose:** Standard CIP-005-4 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability**
 - 4.1. Within the text of Standard CIP-005-4, “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-005-4:
 - 4.2.1 Facilities regulated by 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-002-4, identify that they have no Critical Cyber Assets.~~ 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 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.
5. **Effective Date:** The first day of the ~~third~~eight calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

- R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
 - R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

- R1.2.** For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
 - R1.3.** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
 - R1.4.** Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4.
 - R1.5.** Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
 - R1.6.** The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.
- R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
- R2.1.** These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
 - R2.2.** At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
 - ~~**R2.3.** The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).~~
 - ~~**R2.4.** R2.3. ~~Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.~~~~
 - ~~**R2.5.** R2.4. The required documentation shall, at least, identify and describe:
 - ~~**R2.5.1.** R2.4.1. The processes for access request and authorization.~~
 - ~~**R2.5.2.** R2.4.2. The authentication methods.~~
 - ~~**R2.5.3.** R2.4.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.~~
 - ~~**R2.5.4.** R2.4.4. The controls used to secure dial-up accessible connections.~~~~
 - ~~**R2.6.** R2.5. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.~~

- R3. Monitoring Electronic Access** — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
- R3.1.** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
- R3.2.** Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
- R4. Cyber Vulnerability Assessment** — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
- R4.1.** A document identifying the vulnerability assessment process;
- R4.2.** A review to verify that only ports and services required for operations at these access points are enabled;
- R4.3.** The discovery of all access points to the Electronic Security Perimeter;
- R4.4.** A review of controls for default accounts, passwords, and network management community strings;
- R4.5.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R5. Documentation Review and Maintenance** — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.
- R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.
- R5.2.** The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
- R5.3.** The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R6. Interactive Remote Access Controls — The Responsible Entity that allows interactive remote access to Cyber Asset(s) within its Electronic Security Perimeter(s) shall establish, document, implement and maintain the controls in the following subrequirements:

—Approved by the Board of Trustees

For the purpose of CIP-005-4 Requirement R6:

Interactive remote access is user interactive access by a person, used for support or maintenance, which originates from a Cyber Asset which is not an intermediate device, and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Support or maintenance includes non-operational activities associated with the upkeep, testing and modification of Cyber Assets or networks within the Electronic Security Perimeter. Examples of support or maintenance activities include, but are not limited to, configuration changes, power system model maintenance, vulnerability assessments, incident response, troubleshooting, computer system monitoring, and application of software patches.

R6.1. Implement an intermediate device such that the Cyber Asset initiating interactive remote access does not have direct access to Cyber Asset(s) within the Electronic Security Perimeter.

R6.2. Implement interactive remote access such that communications between the Cyber Asset initiating interactive remote access and the intermediate device are encrypted (encryption for dial-up connections is required only where technically feasible) while using a network that is shared with users not associated with the Responsible Entity.

R6.3. Implement interactive remote access such that multi-factor authentication is required for all interactive remote access between the originating Cyber Asset and the intermediate device, where technically feasible.

R6.4. Establish, document, implement and maintain an interactive remote access user policy, that addresses the following:

- 6.4.1.** Specific language in the interactive login banner on the intermediate device for remote access which requires acknowledgement and adherence to the controls specified interactive remote access user policy, where technically feasible.
- 6.4.2.** Update anti-malware software on Cyber Assets used to initiate the interactive remote access, consistent with CIP-007-4 Requirement R4, before a successful connection is completed
- 6.4.3.** Update patch levels for operating system and applications used to initiate the interactive remote access, consistent with CIP-007-4 Requirement R3, before a successful connection is completed
- 6.4.4.** Prohibit VPN “split-tunneling” or “dual-homed” workstations (which can concurrently access multiple networks) when performing interactive remote access
- 6.4.5.** For vendors, contractors, or consultants: include language in contracts that binds all interactive remote access Cyber Assets to comply with items 6.4.2, 6.4.3 and 6.4.4 of this list.

For the purpose of CIP-005-4 Requirement R6:

An intermediate device is a Cyber Asset that is 1) used to provide the required multi-factor authentication for the interactive remote access; 2) is a termination point for the required encrypted communication; and 3) restricts the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the access control device (firewall) on the Electronic Security Perimeter, or in a DMZ network.

C. Measures

- M1.** The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.
- M2.** The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation of implementation of its interactive remote access controls as specified in Requirement R6. For Requirement R6.4, this is limited reviewing the documented policy only.

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 Entity.
- 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.~~

~~1.3.1.2. Compliance Monitoring and Enforcement Processes~~

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

~~1.4.1.3. Data Retention~~

~~1.4.1.3.1~~ The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

~~1.4.2.1.3.2~~ The Responsible Entity shall keep other documents and records required by Standard CIP-005-4 from the previous full calendar year. The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.5.1.4. Additional Compliance Information~~

2. Violation Severity Levels (~~Developed separately To be added later.~~)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved	Modifications to clarify the requirements and to bring the	Revised.

~~Approved by the Board of Trustees: January 24, 2011~~ 5

Formatted Table

	by NERC Board of Trustees 5/6/09	<p>compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s).</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
<u>3</u>		<u>Update version from -2 to -3</u>	
<u>3</u>	<u>12/16/09</u>	<u>Approved by the NERC Board of Trustees</u>	<u>Update</u>
<u>34</u>	<u>TBD 12/16/09</u>	<p>Changed CIP-005-2 to CIP-005-3.</p> <p>Changed all references to CIP Version “2” standards to CIP Version “3” standards.</p> <p>For Violation Severity Levels, changed, “To be developed later” to “Developed separately.” <u>Modifications to address remote access to Critical Assets for support staff maintenance</u></p>	<p>Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009) <u>8/5/2010</u></p>
<u>45</u>	<u>Board approved 01/24/2011</u>	Update version number from “ <u>-3</u> ” to “ <u>-4</u> ”	<u>Update to conform to changes to CIP-002-4 (Project 2008-06)</u>

Formatted Table

Appendix 4

Requirement Number and Text of Requirement
<p>Section 4.2.2— Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.</p> <p>Requirement R1.3— Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).</p>
Question 1 (Section 4.2.2)
<p>What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?</p>
Response to Question 1
<p>In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.</p>
Question 2 (Section 4.2.2)
<p>Is the communication link physical or logical? Where does it begin and terminate?</p>
Response to Question 2
<p>The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.</p>
Question 3 (Requirement R1.3)
<p>Please clarify what is meant by an "endpoint"? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?</p>
Response to Question 3
<p>The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.</p>
Question 4 (Requirement R1.3)
<p>If "endpoint" is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an "access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal</p>

~~Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?~~

Response to Question 4

~~In the case where the "endpoint" is defined as logical and is \geq layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."~~