

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-4a
3. **Purpose:** Standard CIP-005-4a 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-005-4a 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-005-4a, “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-005-4a:
 - 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.
 - 4.2.4 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.
5. **Effective Date:** The first day of the eighth 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-005-4a.
- 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-005-4a Requirements R2 and R3; Standard CIP-006-4c 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.** 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.** The required documentation shall, at least, identify and describe:
 - R2.5.1.** The processes for access request and authorization.
 - R2.5.2.** The authentication methods.
 - R2.5.3.** The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.
 - R2.5.4.** The controls used to secure dial-up accessible connections.
 - R2.6.** 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. (Retirement approved by FERC effective January 21, 2014.)

- 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-005-4a.
 - R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a 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.

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.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

- 1.2.1** For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- 1.2.1** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 1.2.1** 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.
- 1.2.2** For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

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 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** The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.
- 1.4.3** 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

2. Violation Severity Levels

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|-------------|--------|---|--|---|---|
| R1. | MEDIUM | The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s). | The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s). | The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s). | The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets. |
| R1.1. | MEDIUM | N/A | N/A | N/A | Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s). |
| R1.2. | MEDIUM | N/A | N/A | N/A | For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device. |
| R1.3. | MEDIUM | N/A | N/A | N/A | At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter. |
| R1.4. | MEDIUM | N/A | One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005. | One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005. | One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005. |
| R1.5. | MEDIUM | A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement | A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; | A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of 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; | A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of 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; |

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|-------------|--------|---|---|---|--|
| | | 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. | 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. | and Standard CIP-009-4. | and Standard CIP-009-4. |
| R1.6. | LOWER | N/A | N/A | The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points. | The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points. |
| R2. | MEDIUM | N/A | The Responsible Entity implemented but did not 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). | The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). | The Responsible Entity did not implement nor 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. | MEDIUM | N/A | N/A | N/A | The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified. |
| R2.2. | MEDIUM | N/A | At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security | At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services. | At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services. |

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|--|--------|--|---|--|--|
| | | | Perimeter. | | |
| R2.3. | MEDIUM | N/A | N/A | The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable. | The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable. |
| R2.4. | MEDIUM | N/A | N/A | N/A | Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible. |
| R2.5. | LOWER | The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4 | The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4 | The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4 | The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4 |
| R2.5.1. | LOWER | N/A | N/A | N/A | N/A |
| R2.5.2. | LOWER | N/A | N/A | N/A | N/A |
| R2.5.3. | LOWER | N/A | N/A | N/A | N/A |
| R2.5.4. | LOWER | N/A | N/A | N/A | N/A |
| R2.6. (Retirement approved by FERC effective January 21, 2014.) | LOWER | The Responsible Entity did not maintain a document identifying the content of the banner. OR | Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts. | Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts. | Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts. |

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|-------------|--------|--|---|---|---|
| | | Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts. | | | |
| R3. | MEDIUM | The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points. | The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points. | The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points. | The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points. |
| R3.1. | MEDIUM | The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices. | Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices. | Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices. | Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices. |
| R3.2. | MEDIUM | N/A | N/A | Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate | Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR |

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|-------------|--------|---|---|--|---|
| | | | | notification to designated response personnel. | Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days |
| R4. | MEDIUM | The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s). | The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s). | The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s). | The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5. |
| R4.1. | LOWER | N/A | N/A | N/A | N/A |
| R4.2. | MEDIUM | N/A | N/A | N/A | N/A |
| R4.3. | MEDIUM | N/A | N/A | N/A | N/A |
| R4.4. | MEDIUM | N/A | N/A | N/A | N/A |
| R4.5. | MEDIUM | N/A | N/A | N/A | N/A |
| R5. | LOWER | The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4. | The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4. | The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4. | The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4. |

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|-------------|-------|---|---|--|--|
| R5.1. | LOWER | N/A | The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4. | The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4. | The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually. |
| R5.2. | LOWER | For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change. | For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change. | For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change. | For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change. |
| R5.3. | LOWER | The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days. | The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days. | The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days. | The Responsible Entity retained electronic access logs for less than 45 calendar days. |

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 by NERC Board of Trustees 5/6/09 | <p>Modifications to clarify the requirements and to bring the 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> | Revised. |
| 3 | 12/16/09 | <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.”</p> | Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009) |
| 2a | 02/16/10 | Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010 | Addition |
| 4a | 01/24/11 | Adopted by the NERC Board of Trustees | <p>Update to conform to changes to CIP-002-4 (Project 2008-06)</p> <p>Update version number from “3” to “4a”</p> |
| 4a | 4/19/12 | <p>FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012)</p> <p>Added approved VRF/VSL table to section D.2.</p> | |
| 3a, 4a | 2/7/13 | R2.6 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval. | |

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

| | | | |
|----|----------|---|--|
| 4a | 8/12/13 | FERC Order issued granting an extension of time on CIP V4 Reliability Standards. This order extends the enforcement date from April 1, 2014 to October 1, 2014. | |
| 4a | 11/21/13 | R2.6 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02) | |

Appendix 1

| 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</p> |

owned and managed by the same entity, connected via an encrypted link by properly applied Federal 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."