April 21, 2010

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: ***North American Electric Reliability Corporation,***
Docket No. RM06-22-000

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits this petition in accordance with Section 215(d)(1) of the Federal Power Act ("FPA") and Part 39.5 of the Federal Energy Regulatory Commission's ("FERC") regulations seeking approval for interpretation of Section 4.2.2 ("Applicability") and Requirement R1.3 in FERC-approved NERC Reliability Standard CIP-005-2 — Cyber Security — Electronic Security Perimeter(s), as set forth in **Exhibit A** to this petition. Upon FERC approval, the standard that includes the interpretation will be referred to as CIP-005-2a or CIP-005-3a, whichever version of the standard is in effect at the time of FERC approval.[1] For ease of reference, the interpretation will be referred to as CIP-005-2a in this filing.

[1] At the time this request for interpretation was submitted to NERC, Version 1 of the CIP standards was the FERC-approved version in effect. The request for interpretation was therefore processed referencing CIP-005-1. Since then, CIP-005-2 has been submitted and approved by FERC in the *North American Electric Reliability Corporation*, "Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing," 128 FERC ¶ 61,291 (September 30, 2009). In that Order, FERC noted an effective date of Version 2 of the standards to be April 1, 2010. Additionally, NERC submitted a request for FERC approval of Version 3 of the CIP-002 through CIP-009 standards on

The interpretation was approved by the NERC Board of Trustees on February 16, 2010. NERC requests this interpretation be made effective immediately upon approval by FERC.

NERC's petition consists of the following:

- This transmittal letter;
- A table of contents for the filing;
- A narrative description explaining how the interpretation meets the reliability goal of the standard involved;
- Interpretation of CIP-005-2 Applicability Section 4.2.2 and Requirement R1.3 submitted for approval (**Exhibit A**);
- Reliability Standard CIP-005-2a — Cyber Security — Electronic Security Perimeter(s) that includes the appended interpretation (**Exhibit B1**);
- Reliability Standard CIP-005-3a — Cyber Security — Electronic Security Perimeter(s) that includes the appended interpretation (**Exhibit B2)**;
- The complete development record of the interpretation (**Exhibit C**); and
- A roster of the interpretation development team **(Exhibit D)**.

Please contact the undersigned if you have any questions.

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation

December 29, 2009. On March 31, 2010, FERC approved the CIP Version 3 standards in the *North American Electric Reliability Corporation*, "Order on Compliance," 130 FERC ¶ 61,271 (2010) (March 31, 2010). In that Order, FERC noted an effective date of Version 3 of the standards to be October 1, 2010.The changes in CIP-005-2 and CIP-005-3 relative to Version 1 of CIP-005 are not material to the substance of the interpretation request under consideration. In this regard, NERC will append the requested interpretation to Version 2 or Version 3 of the CIP-005 standard, whichever is in effect at the time of FERC approval of this interpretation, in lieu of Version 1.

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**) Docket No. RM06-22-000)**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF INTERPRETATION TO RELIABILITY STANDARD CIP-005-2— CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), APPLICABILITY SECTION 4.2.2 AND REQUIREMENT R1.3

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

April 21, 2010

TABLE OF CONTENTS

I. Introduction 1

II. Notices and Communications 2

III. Background 3

a. Regulatory Framework 3

b. Basis for Approval of Proposed Interpretation 3

c. Reliability Standards Development Procedure and Interpretation 3

IV. Reliability Standard CIP-005-2a — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3 4

a. Justification for Approval of Interpretation 5

b. Summary of the Reliability Standard Development Proceedings 8

V. Conclusion 10

Exhibit A — Interpretation of Reliability Standard CIP-005-2 — Cyber Security — Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3, Proposed for Approval.

Exhibit B1 — Reliability Standard CIP-005-2a — Cyber Security — Electronic Security Perimeter(s), that includes the appended interpretation.

Exhibit B2 — Reliability Standard CIP-005-3a — Cyber Security — Electronic Security Perimeter(s), that includes the appended interpretation.

Exhibit C — Complete Record of Development of the interpretation for Reliability Standard CIP-005-1a — Cyber Security — Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3.

Exhibit D — Roster of the Interpretation Development Team.

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[2] hereby requests the Federal Energy Regulatory Commission ("FERC") to approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[3] and Section 39.5 of FERC's Regulations, 18 C.F.R. § 39.5, an interpretation to a requirement of a FERC-approved NERC Reliability Standard:

- CIP-005-2 — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3[4]

No modification to the language contained in this specific requirement is being proposed through the interpretation. The NERC Board of Trustees approved the interpretation to Reliability Standard CIP-005-2 — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3 on February 16, 2010. NERC requests that FERC approve the proposed interpretation to CIP-005-2a or CIP-005-3a, to cover the different versions of the standard as they are or become effective, and make it effective immediately upon approval in accordance with FERC's procedures.

---

[2] NERC was certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. FERC certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

[3] 16 U.S.C. 824o.

[4] At the time this request for interpretation was submitted to NERC, Version 1 of the CIP standards was the FERC-approved version in effect. The request for interpretation was therefore processed referencing CIP-005-1. Since then, CIP-005-2 has been submitted and approved by FERC in the *North American Electric Reliability Corporation*, "Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing," 128 FERC ¶ 61,291 (September 30, 2009) ("September 30 Order"). In that Order, FERC noted an effective date of Version 2 of the standards to be April 1, 2010. Additionally, NERC submitted a request for FERC approval of Version 3 of the CIP-002 through CIP-009 standards on December 29, 2009. On March 31, 2010, FERC approved the CIP Version 3 standards in the *North American Electric Reliability Corporation*, "Order on Compliance," 130 FERC ¶ 61,271 (2010) (March 31, 2010) ("March 31 Order"). In that Order, FERC noted an effective date of Version 3 of the standards to be October 1, 2010.The changes in CIP-005-2 and CIP-005-3 relative to Version 1 of CIP-005 are not material to the substance of the interpretation request under consideration. In this regard, NERC will append the requested interpretation to Version 2 or Version 3 of the CIP-005 standard, whichever is in effect at the time of FERC approval of this interpretation, in lieu of Version 1. For ease of reference, the interpretation will be referred to as CIP-005-2a in this filing.

Exhibit A to this filing sets forth the proposed interpretation. **Exhibit B1** contains Reliability Standard CIP-005-2a that includes the appended interpretation. **Exhibit B2** contains Reliability Standard CIP-005-3a that includes the appended interpretation. **Exhibit C** contains the complete development record of the proposed interpretation to CIP-005, Applicability Section 4.2.2 and Requirement R1.3. **Exhibit D** contains a roster of the interpretation development team.

NERC is also filing this interpretation with applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook*
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael*
Assistant General Counsel
Holly A. Hawkins*
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

*Persons to be included on FERC's service list are indicated with an asterisk. NERC requests waiver of FERC's rules and regulations to permit the inclusion of more than two people on the service list.

III. BACKGROUND

a. Regulatory Framework

By enacting the Energy Policy Act of 2005,[5] Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk power system, and with the duties of certifying an electric reliability organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. Section 215 states that all users, owners and operators of the bulk power system in the United States will be subject to FERC-approved Reliability Standards.

b. Basis for Approval of Proposed Interpretation

While this interpretation does not represent a new or modified Reliability Standard requirement, it does provide instruction with regard to the intent and, in some cases, application of the requirement that will guide compliance to it. In this regard, NERC requests that FERC approve this interpretation.

c. Reliability Standards Development Procedure and Interpretation

All persons who are directly or materially affected by the reliability of the North American bulk power system are permitted to request an interpretation of a Reliability Standard, as discussed in NERC's *Reliability Standards Development Procedure,* which is incorporated into the Rules of Procedure as Appendix 3A.[6] Upon request, NERC will assemble a team with the relevant expertise to address the interpretation request and,

---

[5] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005) (16 U.S.C. § 824o).

[6] *See* NERC's *Reliability Standards Development Procedure Version 7*, approved by the NERC Board of Trustees on November 5, 2009, and by FERC on February 5, 2010 ("*Reliability Standards Development Procedure*"), available at http://www.nerc.com/files/Appendix_3A_ReliabilityStandardsDevelopmentProcedure_02052010.pdf.

within 45 days, present the interpretation response for industry ballot. If approved by the ballot pool and the NERC Board of Trustees, the interpretation is appended to the Reliability Standard and filed for approval by FERC and applicable governmental authorities in Canada to be made effective when approved. When the affected Reliability Standard is next substantively revised using the Reliability Standards Development Process, the interpretation will then be incorporated into the Reliability Standard.

The interpretation set out in **Exhibit A** has been developed and approved by industry stakeholders using NERC's *Reliability Standards Development Procedure.* It was approved by the NERC Board of Trustees on February 16, 2010.

IV. Reliability Standard CIP-005-2a — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3

FERC approved Reliability Standard CIP-005-1 in Order No. 706[7], Reliability Standard CIP-005-2 in the September 30 Order (to be effective April 1, 2010), and Reliability Standard CIP-005-3 in the March 31 Order (to be effective October 1, 2010). The present filing includes the Reliability Standard CIP-005-2a that contains the appended interpretation in **Exhibit B1** and the proposed Reliability Standard CIP-005-3a that contains the appended interpretation in **Exhibit B2.**

In Section IV (a), below, NERC discusses the proposed interpretation to the standard, and explains the need for the development of an interpretation to Applicability Section 4.2.2 and Requirement R1.3 in Reliability Standard CIP-005 — Cyber Security — Electronic Security Perimeter(s). In this discussion, NERC demonstrates that the interpretation is consistent with the stated reliability goals of the FERC-approved standard.

[7] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, at PP 24 and 478 (2008).

The complete development record for the interpretation, set forth in **Exhibit C**, includes the request for the interpretation, the response to the request for the interpretation, the ballot pool and the final ballot results by registered ballot body members, stakeholder comments received during the balloting and an explanation of how those comments were considered. **Exhibit D** contains a roster of the team members who worked on the interpretation.

a. Justification for Approval of Interpretation

On February 6, 2009, PacifiCorp, with a shared interest from nine other registered entities, submitted a request for formal interpretation of CIP-005-1 — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirements R1.3. Reliability Standard CIP-005 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."

Section 4.2.2 of CIP-005-2 provides an exception as follows:

> **4.2.** The following are exempt from Standard CIP-005-2:
>
> **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, identify that they have no Critical Cyber Assets.[8]

Requirement R1 of the standard provides:

> **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).

[8] The requirements in R4.2, R4.2.1, R4.2.2, and R4.2.3 of CIP-005-3 are identical to the requirements of the FERC-approved Reliability Standard CIP-005-2.

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-005-2.

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 a specified in Standard CIP-003-2, Standard CIP-004-2 Requirement R3, Standard CIP-005-2 Requirements R2 and R3, Standard CIP-006-2 Requirement R3, Standard CIP-007-2, Requirements R1 and R3 through R9, Standard CIP-008-2, and Standard CIP-009-2.

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.

PacifiCorp requested clarification on a number of issues as outlined below.

Members of the Cyber Security Order No. 706 Standard Authorization Request ("SAR") Standard Drafting Team were assigned to respond to the request and developed the following response to the interpretation requests:

Question 1 (Applicability Section 4.2.2)
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?

Response to Question 1
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.

Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?

Response to Question 2
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.

Question 3 (Requirement R1.3)
Please clarify what is meant by an "endpoint"? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?

Response to Question 3
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.

Question 4 (Requirement R1.3)
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 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 >= 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."

The standard drafting team developed this interpretation consistent with the reliability purpose of the standard, which stipulates that all Critical Cyber Assets be

protected, drawing a careful distinction between assets external to the Electronic Security Perimeter referenced in Applicability Section 4.2.2 and those with endpoints on or within the Electronic Security Perimeter. In this context, the interpretation represents a response consistent with the intended objective of the standard. The protection of these assets starts with the identification of a perimeter that circumscribes the Critical Cyber Assets, referred to as an Electronic Security Perimeter, as well as all access points to the perimeter, and the assets within it.

b. Summary of the Reliability Standard Development Proceedings

PacifiCorp submitted the request for interpretation of CIP-005-1 — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3 on February 6, 2009. NERC presented the interpretation response for pre-ballot review on July 27, 2009. The initial ballot was conducted from August 27, 2009 through September 8, 2009 and achieved a quorum of 84.68 percent with a weighted affirmative approval of 80.37 percent. There were 45 negative ballots submitted for the initial ballot, and 30 of those ballots included a comment, which initiated the need for a recirculation ballot.

The recirculation ballot was conducted from October 16, 2009 through October 26, 2009, and achieved a quorum of 86.29 percent with a weighted affirmative approval of 83.25 percent. There were 41 negative ballots submitted for the recirculation ballot, and 29 of those ballots included a comment. Some balloters listed more than one reason for their negative ballot.

There were mainly two themes that the commenters raised. First, there were comments that pertain to lack of clarity around the issue of access point identification.

Second, some commenters questioned the interpretation on tunnels that have termination point beyond an Electronic Security Perimeter (ESP) access point.

More specifically, the reasons cited for the negative ballots included the following:

- Seventeen balloters indicated the interpretation either did not provide sufficient clarity or raised more questions; as follows:
  - Eight balloters sought more information regarding what constitutes an "endpoint" or the communication link's termination points. One suggested the interpretation should state the termination points depend on design and architecture and could include at least three common design examples.
  - Four balloters asked how control could be better than a six-wall border.
  - Three balloters sought more information about "data communication links."
  - Two balloters gave an example that in the response to question 4, there is discussion relative to layers 3 and higher, but nothing mentioned for layers 1 or 2.
  - One balloter asked if the communication link was meant to be physical or logical.
- Thirteen balloters indicated concerns with the answer to question 4:
  - Four balloters indicated the firewall access points already enforce port/protocol restrictions, which meet the requirement, stating that "[a]dding the further restriction of access points at the encryption endpoint is unnecessary, increases complexity which by definition reduces reliability, and can have much wider implications beyond encrypted tunnels."
  - Four balloters indicated wording in the response that "the termination points of an encrypted tunnel must be treated as an 'access point'" is too restrictive and will conflict with other interpretations, specifically PacifiCorp's request for interpretation of CIP-006-1. The balloters were concerned that the interpretation could be viewed as indicating all encrypted tunnels are an access point to an ESP.
  - Three balloters indicated that "[a] distinction has to be made in the response in regards to the encryption tunnel termination point when deciding whether such termination point is treated as an 'access point' or not."
  - One balloter stated that virtual private network ("VPN") traffic should be treated the same as any other logical connection and that the access point to the ESP is able to provide layer 3 and 4 protection regardless of the type of traffic being traversed.

- One balloter indicated the question is confusing but believes the intent is to clarify that "access points" to an ESP can be effectively moved with the application of appropriate equipment. The balloter stated that a communication link between two ESPs utilizing an encrypted tunnel must have an encryption/decryption device at each end inside the ESP that would be defined as the "termination point." The balloter asked, "if an additional protective device is added before the 'termination point' to protect the ESP, would this not affectively move the 'access point?' Must the logs of both protective devices be maintained?"

- One balloter disagreed with the response to question 3 regarding logical communication links, stating it could be taken to mean that any device at which a logical connection into the ESP terminates would be considered an access point.

In response, the standard drafting team clarified that an encrypted tunnel that originates from outside of the ESP and terminates within or at the ESP is an access point. With regard to tunnels that have a termination point beyond an ESP access point, the standard drafting team responded that encrypted data cannot be adequately inspected at an upstream access point, such as a firewall, in order to provide the required level of protection; and that on that basis the termination point must be considered an access point to the ESP and must be protected per CIP-005.

V. CONCLUSION

NERC respectfully requests that FERC approve the interpretation to FERC-approved Reliability Standard CIP-005-2 — Cyber Security — Electronic Security Perimeter(s) (and CIP-005-3, for when it becomes effective), Applicability Section 4.2.2 and Requirement R1.3, as set out in **Exhibit A**, in accordance with Section 215(d)(1) of the FPA and Part 39.5 of FERC's regulations. NERC requests that this interpretation be made effective immediately upon issuance of FERC's order in this proceeding.

Respectfully submitted,

/s/ Holly A. Hawkins

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 21st day of April, 2010.

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation

Exhibit A

Interpretation of Reliability Standard CIP-005-2 — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3 Proposed for Approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard
Date submitted: 02/06/09
Contact information for person requesting the interpretation:
Name: Daniel Marvin
Organization: PacifiCorp
Telephone: 503.813.5375
E-mail: daniel.marvin@pacificorp.com
Identify the standard that needs clarification:
Standard Number: CIP-005-1
Standard Title: Cyber Security -- Electronic Security Perimeters
Identify specifically what needs clarification (If a category is not applicable, please leave it blank)**:**

Requirement Number and Text of Requirement: CIP-005-1 4.2.2 and R1.3

4.2. The following are exempt from Standard CIP-005:

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

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).

Clarification needed:

4.2.2 indicates that the communication links between ESPs and the required supporting equipment are not in the scope of this standard. However, in R1.3, the endpoints of a communication link between ESPs are required to be treated as "access points".

Regarding 4.2.2:

- 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?
- Is the communication link physical or logical? Where does it begin and terminate?

Regarding R1.3:

- Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?

Request for an Interpretation of a Reliability Standard
• 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 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?
Identify the material impact associated with this interpretation:
The material impact is potential non-compliance with the standard as written. Many utilities have multiple control centers with fail over features between the facilities, and the communication links protected by encryption mechanisms such as VPN. Requiring all VPN termination points to also be access points introduces the requirement for strong authentication at the access point, increases complexity in network access controls and thus heightens probabilities of unintended failures, and will negatively impact real-time fail over functionality between control centers. In addition, PacifiCorp is concerned regarding potential conflict with the published answer to Question #15, in the CIP-002-009 FAQ, "*Encryption or other data integrity checking technologies can also ensure that data is not changed in transit...*" **The following industry entities have a shared interest with PacifiCorp in this clarification request:** • Idaho Power • Puget Sound Energy • Platte River Power Authority • Eugene Water & Electric Board • Seattle City Light • Arizona Public Service • Bonneville Power Administration • TransAlta • Xcelenergy

Project 2009-12: Response to Request for an Interpretation of CIP-005-1 Section 4.2.2 and Requirement R1.3 for PacifiCorp
The following interpretation of CIP-005-1 — Cyber Security — Electronic Security Perimeters was developed by the Cyber Security Order 706 SAR drafting team.
Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **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).
Question 1 (Section 4.2.2)
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?
Response to Question 1
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.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
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.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3

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.
Question 4 (Requirement R1.3)
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 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 >= 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.”

Exhibit B1

Reliability Standard CIP-005-2a — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3 that includes the Appended Interpretation
(Clean and Redline)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-2a

3. Purpose: Standard CIP-005-2 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-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "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-005-2:

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, 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 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-005-2.

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 a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

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-004-2 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.

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-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 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-008-2.

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

1.1.1 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. 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-008-2, 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-005-2 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 (To be developed 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		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. 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). Changed compliance monitor to Compliance Enforcement Authority.	
2	05/06/09	Adopted by NERC Board of Trustees	Revised
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010.	Addition

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **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).
Question 1 (Section 4.2.2)
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?
Response to Question 1
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.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
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.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
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.
Question 4 (Requirement R1.3)
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 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 >= 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.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-2a

3. Purpose: Standard CIP-005-2 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-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "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-005-2:

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, 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 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-005-2.

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 a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

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-004-2 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.

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-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 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-008-2.

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

1.1.1 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. 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-008-2, 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-005-2 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 (To be developed 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		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. 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). Changed compliance monitor to Compliance Enforcement Authority.	
2	05/06/09	Adopted by NERC Board of Trustees	Revised
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010.	Interpretation

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **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).
Question 1 (Section 4.2.2)
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?
Response to Question 1
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.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
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.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
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.
Question 4 (Requirement R1.3)
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 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 >= 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.”

Exhibit B2

Reliability Standard CIP-005-3a — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3 that includes the Appended Interpretation
(Clean and Redline)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-3a

3. Purpose: Standard CIP-005-3 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-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability

4.1. Within the text of Standard CIP-005-3, "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-005-3:

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-002-3, 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 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-005-3.

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 a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

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-004-3 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.

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-005-3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 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-008-3.

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

1.1.1 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. 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-008-3, 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-005-3 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 (To be developed 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		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. 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). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **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).
Question 1 (Section 4.2.2)
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?
Response to Question 1
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.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
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.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
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.
Question 4 (Requirement R1.3)
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 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 >= 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.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-3a

3. Purpose: Standard CIP-005-3 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-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability

4.1. Within the text of Standard CIP-005-3, "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-005-3:

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-002-3, 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 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-005-3.

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 a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

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-004-3 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.

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-005-3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 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-008-3.

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

1.1.1 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. 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-008-3, 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-005-3 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 (To be developed 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		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. 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). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **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).
Question 1 (Section 4.2.2)
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?
Response to Question 1
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.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
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.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
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.
Question 4 (Requirement R1.3)
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 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 >= 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.”

Exhibit C

Complete Record of Development of the Interpretation for Reliability Standard CIP-005-1a — Cyber Security — Electronic Security Perimeter(s), Applicability Section 4.2.2 and Requirement R1.3

Project 2009-12
Interpretation – CIP-005-1 – Cyber Security – Electronic Security Perimeters by PacifiCorp

Status:
The interpretation was approved by the NERC Board of Trustees on February 16, 2010.

Summary: The request asks to clarify the following:

- 4.2.2 indicates that the communication links between ESPs and the required supporting equipment are not in the scope of this standard. However, in R1.3, the endpoints of a communication link between ESPs are required to be treated as "access points".
- Regarding 4.2.2:
- 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?
- Is the communication link physical or logical? Where does it begin and terminate?
- Regarding R1.3:
- Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
- 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 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?

Interpretation Process: In accordance with the Reliability Standards Development Procedure, the interpretation must be posted for a 30-day pre-ballot review, and then balloted. There is no public comment period for an interpretation. Balloting will be conducted following the same method used for balloting standards. If the interpretation is approved by its ballot pool, then the interpretation will be appended to the standard and will become effective when adopted by the NERC Board of Trustees and approved by the applicable regulatory authorities. The interpretation will remain appended to the standard until the standard is revised through the normal standards development process. When the standard is revised, the clarifications provided by the interpretation will be incorporated into the revised standard.

Draft	Action	Dates	Results	Consideration of Comments
PacifiCorp Request for Interpretation of CIP-005-1 Interpretation **(2)** Request for Interpretation **(1)**	Recirculation Ballot Info>> **(8)** | Vote>>	10/16/09 - 10/26/09 (closed)	Summary>> **(9)** Full Record>> **(10)**	
	Initial Ballot Info>> **(4)** | Vote>>	08/27/09 - 09/08/09 (closed)	Summary>> **(5)** Full Record>> **(6)**	Consideration of Comments>> **(7)**
	Pre-ballot Review Info>> **(3)** | Join>>	07/27/09 - 08/27/09 (closed)		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard
Date submitted: 02/06/09
Contact information for person requesting the interpretation:
Name: Daniel Marvin
Organization: PacifiCorp
Telephone: 503.813.5375
E-mail: daniel.marvin@pacificorp.com
Identify the standard that needs clarification:
Standard Number: CIP-005-1-4.2.2 and CIP-005-1-R1.3
Standard Title: CIP-005-1 --Cyber Security -- Electronic Security Perimeters
Identify specifically what needs clarification:

Request for an Interpretation of a Reliability Standard

Requirement Number and Text of Requirement: **CIP-005-1 4.2.2 and R1.3**

4.2. The following are exempt from Standard CIP-005:

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.

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).

Clarification needed:

4.2.2 indicates that the communication links between ESPs and the required supporting equipment are not in the scope of this standard. However, in R1.3, the endpoints of a communication link between ESPs are required to be treated as "access points".

Regarding 4.2.2:

- 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?
- Is the communication link physical or logical? Where does it begin and terminate?

Regarding R1.3:

- Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
- 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 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?

Identify the material impact associated with this interpretation:

Request for an Interpretation of a Reliability Standard

The material impact is potential non-compliance with the standard as written.

Many utilities have multiple control centers with fail over features between the facilities, and the communication links protected by encryption mechanisms such as VPN. Requiring all VPN termination points to also be access points introduces the requirement for strong authentication at the access point, increases complexity in network access controls and thus heightens probabilities of unintended failures, and will negatively impact real-time fail over functionality between control centers.

In addition, PacifiCorp is concerned regarding potential conflict with the published answer to Question #15, in the CIP-002-009 FAQ, "*Encryption or other data integrity checking technologies can also ensure that data is not changed in transit...*"

The following industry entities have a shared interest with PacifiCorp in this clarification request:

- Idaho Power
- Puget Sound Energy
- Platte River Power Authority
- Eugene Water & Electric Board
- Seattle City Light
- Arizona Public Service
- Bonneville Power Administration
- TransAlta
- Xcelenergy

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard
Date submitted: 02/06/09
Contact information for person requesting the interpretation:
Name: Daniel Marvin
Organization: PacifiCorp
Telephone: 503.813.5375
E-mail: daniel.marvin@pacificorp.com
Identify the standard that needs clarification:
Standard Number: CIP-005-1
Standard Title: Cyber Security -- Electronic Security Perimeters
Identify specifically what needs clarification (If a category is not applicable, please leave it blank)**:**

Requirement Number and Text of Requirement: CIP-005-1 4.2.2 and R1.3

4.2. The following are exempt from Standard CIP-005:
4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

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).

Clarification needed:

4.2.2 indicates that the communication links between ESPs and the required supporting equipment are not in the scope of this standard. However, in R1.3, the endpoints of a communication link between ESPs are required to be treated as "access points".

Regarding 4.2.2:

- 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?
- Is the communication link physical or logical? Where does it begin and terminate?

Regarding R1.3:

- Please clarify what is meant by an “endpoint”? Is it physical termination? Logical

Request for an Interpretation of a Reliability Standard

termination of OSI layer 2, layer 3, or above?

- 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 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?

Identify the material impact associated with this interpretation:

The material impact is potential non-compliance with the standard as written.

Many utilities have multiple control centers with fail over features between the facilities, and the communication links protected by encryption mechanisms such as VPN. Requiring all VPN termination points to also be access points introduces the requirement for strong authentication at the access point, increases complexity in network access controls and thus heightens probabilities of unintended failures, and will negatively impact real-time fail over functionality between control centers.

In addition, PacifiCorp is concerned regarding potential conflict with the published answer to Question #15, in the CIP-002-009 FAQ, "*Encryption or other data integrity checking technologies can also ensure that data is not changed in transit…*"

The following industry entities have a shared interest with PacifiCorp in this clarification request:

- Idaho Power
- Puget Sound Energy
- Platte River Power Authority
- Eugene Water & Electric Board
- Seattle City Light
- Arizona Public Service
- Bonneville Power Administration
- TransAlta
- Xcelenergy

Project 2009-12: Response to Request for an Interpretation of CIP-005-1 Section 4.2.2 and Requirement R1.3 for PacifiCorp

The following interpretation of CIP-005-1 — Cyber Security — Electronic Security Perimeters was developed by the Cyber Security Order 706 SAR drafting team.

Requirement Number and Text of Requirement

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

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).

Question 1 (Section 4.2.2)

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?

Response to Question 1

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.

Question 2 (Section 4.2.2)

Is the communication link physical or logical? Where does it begin and terminate?

Response to Question 2

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.

Question 3 (Requirement R1.3)

Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?

Response to Question 3

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.

Question 4 (Requirement R1.3)
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 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 >= 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.”

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool and Pre-ballot Window
July 27–August 27, 2009

Now available at: https://standards.nerc.net/BallotPool.aspx

Project 2009-12: Interpretation of CIP-005-1 for PacifiCorp

An interpretation of standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s) Section 4.2.2 and Requirement R1.3 for PacifiCorp is posted for a 30-day pre-ballot review. Registered Ballot Body members may join the ballot pool to be eligible to vote on this interpretation **until 8 a.m. EDT on August 27, 2009**.

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list server for this ballot pool is: bp-2009-12_RFI_CIP-005_in@nerc.com.

Next Steps

Voting will begin shortly after the pre-ballot review closes.

Project Background

PacifiCorp requested clarification on the meaning of "associated" cyber assets referenced in Section 4.2.2, the meaning of "endpoint" in Requirement R1.3, and the relationship of an endpoint and an "access point."

The request and interpretation can be found on the project page:
http://www.nerc.com/filez/standards/Project2009-12_Interpretation_CIP-005-1_PacifiCorp.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Initial Ballot Window Open

August 27–September 8, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Project 2009-12: Interpretation of CIP-005-1 for PacifiCorp

An initial ballot window for an interpretation of standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s) Section 4.2.2 and Requirement R1.3 for PacifiCorp is now open **until 8 p.m. EDT on September 8, 2009**.

Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

PacifiCorp requested clarification on the meaning of "associated" cyber assets referenced in Section 4.2.2, the meaning of "endpoint" in Requirement R1.3, and the relationship of an endpoint and an "access point."

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2009-12_Interpretation_CIP-005-1_PacifiCorp.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Initial Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Project 2009-12: Interpretation of CIP-005-1 for PacifiCorp
The initial ballot for an interpretation of standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s) Section 4.2.2 and Requirement R1.3 for PacifiCorp ended September 8, 2009.

Ballot Results
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 84.6 8%
Approval: 80.3 7%

Since at least one negative ballot included a comment, these results are not final. A second (or recirculation) ballot must be conducted. Ballot criteria details are listed at the end of the announcement.

Next Steps
As part of the recirculation ballot process, the drafting team must draft and post responses to voter comments. The drafting team will also determine whether or not to make revisions to the balloted item(s). Should the team decide to make revisions, the revised item(s) will return to the initial ballot phase.

Project Background
PacifiCorp requested clarification on the meaning of "associated" cyber assets referenced in Section 4.2.2, the meaning of "endpoint" in Requirement R1.3, and the relationship of an endpoint and an "access point."

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2009-12_Interpretation_CIP-005-1_PacifiCorp.html

Standards Development Process
The *Reliability Standards Development Procedure* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria
Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results

Ballot Name:	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1_in
Ballot Period:	8/27/2009 - 9/8/2009
Ballot Type:	Initial
Total # Votes:	210
Total Ballot Pool:	248
Quorum:	**84.68 % The Quorum has been reached**
Weighted Segment Vote:	80.37 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	67	1	33	0.717	13	0.283	8	13
2 - Segment 2.	10	0.7	6	0.6	1	0.1	2	1
3 - Segment 3.	59	1	39	0.813	9	0.188	2	9
4 - Segment 4.	11	1	9	0.9	1	0.1	0	1
5 - Segment 5.	45	1	24	0.667	12	0.333	3	6
6 - Segment 6.	33	1	19	0.731	7	0.269	2	5
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.5	4	0.4	1	0.1	1	2
9 - Segment 9.	8	0.6	5	0.5	1	0.1	1	1
10 - Segment 10.	7	0.7	7	0.7	0	0	0	0
Totals	**248**	**7.5**	**146**	**6.028**	**45**	**1.473**	**19**	**38**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Avista Corp.	Scott Kinney	Abstain	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Negative	View

1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	E.ON U.S. LLC	Larry Monday		
1	East Kentucky Power Coop.	George S. Carruba		
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Abstain	View
1	ITC Transmission	Elizabeth Howell	Negative	
1	JEA	Ted E. Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Kissimmee Utility Authority	Joe B Watson		
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	Rodney Hawkins		
1	Lincoln Electric System	Doug Bantam		
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	National Grid	Manuel Couto		
1	Nebraska Public Power District	Richard L. Koch	Abstain	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Negative	
1	Pacific Gas and Electric Company	Chifong L. Thomas		
1	PacifiCorp	Mark Sampson		
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Negative	View
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Puget Sound Energy, Inc.	Catherine Koch		
1	Salt River Project	Robert Kondziolka	Negative	View
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SaskPower	Wayne Guttormson	Abstain	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Abstain	
1	Southern California Edison Co.	Dana Cabbell	Negative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Negative	View
1	Tampa Electric Co.	Thomas J. Szelistowski	Abstain	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L. Pieper	Negative	View
2	Alberta Electric System Operator	Jason L. Murray	Abstain	
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Abstain	

2	New Brunswick System Operator	Alden Briggs		
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Affirmative	
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana		
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Black Hills Power	Andy Butcher	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	City of Farmington	Linda R. Jacobson		
3	City Public Service of San Antonio	Edwin Les Barrow	Affirmative	
3	Colorado Springs Utilities	Alan Laborwit	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	View
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	East Kentucky Power Coop.	Sally Witt	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W Pourciau	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory David Woessner		
3	Lakeland Electric	Mace Hunter		
3	Lincoln Electric System	Bruce Merrill	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C Parent	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	Mark Alberter	Negative	View
3	Salt River Project	John T. Underhill	Negative	View
3	San Diego Gas & Electric	Scott Peterson		
3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Negative	View
3	Tampa Electric Co.	Ronald L. Donahey		
3	Wisconsin Electric Power Marketing	James R. Keller	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	View
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt		
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	

4	Northern California Power Agency	Fred E. Young	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Calpine Corporation	John Brent Hebert		
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consumers Energy	James B Lewis		
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Robert Smith	Negative	View
5	Dynegy	Greg Mason	Negative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	View
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	Kansas City Power & Light Co.	Scott Heidtbrink	Negative	View
5	Lakeland Electric	Thomas J Trickey	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin	Affirmative	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	Michigan Public Power Agency	James R. Nickel	Affirmative	View
5	MidAmerican Energy Co.	Christopher Schneider	Abstain	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp Energy	David Godfrey	Negative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PPL Generation LLC	Mark A. Heimbach	Negative	View
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik		
5	RRI Energy	Thomas J. Bradish	Negative	View
5	Salt River Project	Glen Reeves	Negative	View
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	South California Edison Company	Ahmad Sanati		
5	South Carolina Electric & Gas Co.	Richard Jones	Affirmative	
5	Tampa Electric Co.	Frank L Busot	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Eugene Water & Electric Board	Daniel Mark Bedbury	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Thomas Saitta	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	

6	Louisville Gas and Electric Co.	Daryn Barker	Affirmative	
6	Luminant Energy	Thomas Burke		
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PacifiCorp	Gregory D Maxfield	Negative	
6	Portland General Electric Co.	John Jamieson		
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Negative	View
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Southern California Edison Co.	Marcus V Lotto	Negative	View
6	Tampa Electric Co.	Joann Wehle		
6	Western Area Power Administration - UGP Marketing	John Stonebarger	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Negative	View
8	Edward C Stein	Edward C Stein	Negative	
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Abstain	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz		
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
8	Wally Magda	Wally Magda	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	View
9	Public Service Commission of South Carolina	Philip Riley	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Negative	
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	View
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2009-12: Interpretation of CIP-005-1 — Cyber Security — Electronic Security Perimeters for PacifiCorp
Consideration of Comments on Initial Ballot (August 27–September 8, 2009)

Summary Consideration:

There were mainly two themes that the commenters raised. First, there were comments that pertain to lack of clarity around the issue of access point identification. Second, some commenters questioned the interpretation on tunnels that have termination point beyond an Electronic Security Perimeter (ESP) access point.

The drafting team response to the first theme clarifies that an encrypted tunnel that originates from outside of the ESP and terminates within or at the ESP is an access point. The drafting team offers that encrypted data cannot be adequately inspected at an upstream access point, such as a firewall, in order to provide the required level of protection. Therefore, the termination point must be considered an access point to the ESP and must be protected per CIP-005.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Voter	Entity	Segment	Vote	Comment
James L. Jones	Southwest Transmission Cooperative, Inc.	1	Negative	A distinct lack of clarity around the characteristics of an "endpoint" and what devices are in scope as being associated with "data communication links". Unfortunately, the proposed interpretation provides no meaningful clarity.The interpretation is still hazy in my mind.
Response1: Thank you for your comment. 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.				
Donald S. Watkins	Bonneville Power Administration	1	Negative	BPA believes the interpretation wording of Question 4 that "the termination points of an encrypted tunnel must be treated as an "access point"" is too restrictive and will conflict with other interpretations. Specifically the PACW request for interpretation of CIP-006-

[1] The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

Voter	Entity	Segment	Vote	Comment
Rebecca Berdahl	Bonneville Power Administration	3	Negative	01, the use of data encryption as an alternate measure for physical protection, is meant to allow creating one ESP that spans multiple PSPs. With this CIP-005-01 interpretation, it could be interpreted that all encrypted tunnels are an access point to an ESP. BPA provides the following non-directive comment in regard to the scenario given in Question 4: if the encrypted tunnel is connecting two discrete ESPs, then the ends of link (logical or physical) must be considered access points in accordance with CIP-005-1 R1.1. However, the architecture described in the question could also be interpreted as a single ESP consisting of the individual ESPs at each control center and the link connecting them. In this case, the encryption serves to provide an alternative means of physical protection, as described in the response to Pacificorp's Request for Interpretation for CIP-006-1 . The encrypted link is entirely internal to the PSP and the ESP; and CIP-005 is not relevant. No endpoints exist.
Francis J. Halpin	Bonneville Power Administration	5	Negative	
Brenda S. Anderson	Bonneville Power Administration	6	Negative	
Response2: Thank you for your comment. The encrypted tunnel envisioned as an alternative protective measure for CIP-006-1 extends a single ESP across two geographically separate Physical Security Perimeters (PSPs). In that instance, as the encrypted tunnel is a closed link between the two PSPs and all traffic across that tunnel is contained within a single ESP, the tunnel endpoints would not be considered ESP access points. However, the question asked in this interpretation request is in regard to an encrypted tunnel connecting two distinct ESPs without respect to any PSP containment. In this instance, the endpoints of the encrypted tunnel are the access points to the respective ESPs and must be protected per the requirements of CIP-005-1.				
Russell A Noble	Cowlitz County PUD	3	Negative	Cowlitz PUD votes negative for the following reasons: Answer to Question 2 fails to clarify where a communication link begins and terminates. Cowlitz understands a communication link can be physical and/or logical. However, the interpretation needs to go further than stating the termination points depend on design and architecture. At the very least, three common design scenarios could be explored and termination points defined in each example. Without some guidance, entities are left to guess and hope the auditor will agree. Question 4 is confusing, but Cowlitz believes the intent is to clarify that “access points” to an ESP can be effectively moved with the application of appropriate equipment. A communication link between two ESPs utilizing an encrypted tunnel must have an encryption/decryption device at each end inside the ESP, this is defined as the “termination point”. However, if an additional protective device is added before the “termination point” to protect the ESP, would this not affectively move the “access point?” Must the logs of both protective devices be maintained?
Response3: Thank you for your comment. The drafting team could not be more prescriptive given the language in the standard. While it is true that the design and architecture will determine the endpoints, providing specific examples may unintentionally lead to perceived additional requirements that do not exist in the standard. In regard to your second comment, the insertion of an additional protective device ahead of the tunnel endpoint does not necessarily make that device an access				

Voter	Entity	Segment	Vote	Comment
point for purposes of the tunneled traffic because it cannot enforce access control and monitoring for the contents of that tunnel; it depends also on any other functions the protective device is performing. It may still be considered an access point for the ESP depending on the design and architecture.				
Mark Alberter	Sacramento Municipal Utility District	3	Negative	Further clarification for Q2: Is the communication link physical or logical? Where does it begin and terminate? is required. Specific guidelines identifying the physical or logical links should be identified.
Response4: Thank you for your comment. The drafting team interprets that the communication links could be either physical or logical and whether their endpoints are access points or not depends on the design and architecture.				
Michael Gammon	Kansas City Power & Light Co.	1	Negative	It is difficult or impossible to determine if a control is equivalent or better than a completely enclosed six wall border. This interpretation creates more ambiguity in the standard.
Charles Locke	Kansas City Power & Light Co.	3	Negative	
Thomas Saitta	Kansas City Power & Light Co.	6	Negative	
Response5: Thank you for your comment. This comment may have been intended for the PacifiCorp request for an interpretation of CIP-006 (Project 2009-13).				
Scott Heidtbrink	Kansas City Power & Light Co.	5	Negative	not clear if a control is equiv or better than a 6 wall border
Response6: Thank you for your comment. This comment may have been intended for the PacifiCorp request for an interpretation of CIP-006 (Project 2009-13).				

Voter	Entity	Segment	Vote	Comment
Tom Bowe	PJM Interconnection, L.L.C.	2	Negative	o In response to Q1: PJM has no concerns over this interpretation. o In response to Q2: PJM has no comments. This question and its answer are vague. o In response to Q3: PJM does not have concerns about this response as far as it refers to physical communication link termination; however, with regard to logical communication links, this could be taken to mean that any device at which a logical connection into the ESP terminates, would be considered an access point. PJM disagrees with this interpretation. o In response to Q4: PJM disagrees with this interpretation. VPN traffic should not be considered as different from any other logical connection. The access point to the ESP is able to provide layer 3 and 4 protection regardless of the type of traffic that is being traversed.
Response7: Thank you for your comments. The drafting team interprets a communication link that originates from outside of the ESP and terminates within or at the ESP is an access point (physical or logical). An encrypted tunnel that originates from outside of the ESP and terminates within or at the ESP is an access point. The drafting team offers that encrypted data cannot be adequately inspected at an upstream access point, such as a firewall, in order to provide the required level of protection. Therefore, the termination point must be considered an access point to the ESP and must be protected per CIP-005.				
Robert Smith	Duke Energy	5	Negative	Per the response provided by the Cyber Security Order 706 SAR Drafting team to Question #4, in such instance where a Layer 3 encryption tunnel is deployed between two NERC CIP ESPs (electronic security perimeters), the termination points of such tunnels would need to be considered “access points” and thus NERC CIP requirement CIP 005 R2 would apply in its entirety to these termination points. A distinction has to be made in the response in regards to the encryption tunnel termination point when deciding whether such termination point is treated as an “access point” or not. 1. If a tunnel terminates in front of a Layer 3 filtering device and the traffic is passed through the Layer 3 filtering device in clear text, then the Layer 3 filtering device should be regarded as an “access point” as opposed to the encryption tunnel’s termination point being an “access point”. In this case the Layer 3 filtering device is capable of performing its access control function and is not processing any encrypted data. 2. If a tunnel terminates after passing encrypted traffic through a Layer 3 filtering device, then the Layer 3 filtering device’s capability of data traffic filtering is severely reduced and therefore the tunnel termination point should be treated as an “access point”.
Douglas E. Hils	Duke Energy Carolina	1	Negative	
Henry Ernst-Jr	Duke Energy Carolina	3	Negative	
Response8: Thank you for your comment. The drafting team agrees with your comment that the termination point in your first example is not an access point. Subsequent clarification from PacifiCorp indicated that the tunnel terminated inside the ESP. In regard to your second example, the drafting team again agrees with you. The insertion of an additional protective device ahead of the tunnel endpoint does not				

Voter	Entity	Segment	Vote	Comment
necessarily make that device an access point for purposes of the tunneled traffic because it cannot enforce access control and monitoring for the contents of that tunnel; it depends also on any other functions the protective device is performing. It may still be considered an access point for the ESP depending on the design and architecture.				
Thomas J. Bradish	RRI Energy	5	Negative	RRI Energy votes negative in support of PacifiCorps position namely: PacifiCorp's primary concern was a distinct lack of clarity around the characteristics of an "endpoint" and what devices are in scope as being associated with "data communication links". Unfortunately, the proposed interpretation provides no meaningful clarity. PacifiCorp recommends that entities not support this provided interpretation.
Response9: Thank you for your comment. 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. The drafting team consulted with PacifiCorp in order to understand the specific details of its concern, and we believe the interpretation of the standard addresses PacifiCorp's specific situation.				
Robert Kondziolka	Salt River Project	1	Negative	SRP has specific concerns with the answer to question 4 within the Interpretation. The Firewall access points already enforce port/protocol restrictions which meet the requirement. Adding the further restriction of access points at the encryption endpoint is unnecessary, increases complexity which by definition reduces reliability, and can have much wider implications beyond encrypted tunnels.
John T. Underhill	Salt River Project	3	Negative	
Glen Reeves	Salt River Project	5	Negative	
Mike Hummel	Salt River Project	6	Negative	
Response10: Thank you for your comment. The firewall access point ahead of the tunnel endpoint does not make that upstream device an access point because it cannot enforce access control and monitoring for the contents of that tunnel. Terminating the tunnel immediately before the firewall would allow the firewall to provide the required level of access control and monitoring and would not increase complexity.				
Marcus V Lotto	Southern California Edison Co.	6	Negative	The concern with the Proj. 2009-12 interpretation is the lack of clarity around the characteristics of an "endpoint" and what devices are in scope as being associated with "data communication links". Unfortunately, the proposed interpretation provides no meaningful clarity.
Response11: Thank you for your comment. 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,				

Voter	Entity	Segment	Vote	Comment
irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.				
Fred E. Young	Northern California Power Agency	4	Negative	The interpretation does not provide any additional clarity.
Response12: Thank you for your comment. 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.				
Ray Mammarella	PP&L, Inc.	1	Negative	The interpretation provides minimal clarification based on the questions posed, including prior, similar requests for interpretation. This raises more questions in a complex area where many entities seem to be looking for clear definition and differentiation of terms such as access points and endpoints for their specific, varied, and arguably secure, network design/architectural configurations. For example in the response to Question 4 there is discussion relative to Layers 3 and higher, but there is nothing said for Layer 1 or 2.
Mark A. Heimbach	PPL Generation LLC	5	Negative	
Response13: Thank you for your comment. 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. In response to latter part of your comment, tunnels that are layer 1 or 2 effectively create a single ESP.				
Martin Bauer	U.S. Bureau of Reclamation	5	Negative	The Interpretation with respect to Question 4, implies that use of encryption is not suitable means of protection for access. If an encrypted tunnel is used between two ESP's, it would appear that the encryption itself would ensure restricted access and therefore any aspect of the communication would be secure.
Response14: Thank you for your comment. The interpretation does not imply that encryption is inadequate to provide some level of protection for access. The interpretation clarifies that endpoints, on or inside an ESP, to an encrypted tunnel that originates from outside of an ESP are access points and are subject to CIP-005.				
Gregory L. Pieper	Xcel Energy, Inc.	1	Negative	The language in response to question 2 does not provide any clarity as to what constitutes a communication link's termination points.
David F.	Xcel Energy,	6	Negative	

Voter	Entity	Segment	Vote	Comment
Lemmons	Inc.			
Michael Ibold	Xcel Energy, Inc.	3	Negative	See Xcel Energy Transmission comments.
Response15: Thank you for your comment. 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.				
David Schiada	Southern California Edison Co.	3	Negative	The proposed interpretation does not provide sufficient clarity around the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links”.
Response16: Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The drafting team interprets that either physical or logical data communications links are included and whether their endpoints are access points or not depends on the design and architecture.				
Terry Harbour	MidAmerican Energy Co.	1	Negative	The proposed interpretation provides no meaningful clarity.
Response17: Thank you for your comment. 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.				
James R. Nickel	Michigan Public Power Agency	5	Affirmative	As written, the response is appropriate. However, MPPA suggests that two distinct ESP's owned by a single entity and connected by a secured VPN should be considered a single ESP. This issue should be revisited by the Standards Drafting Team during writing of the Version 3 Standards.
Response18: Thank you for your comment. The drafting team agrees with your suggestion and offers that such a topology can be considered a single ESP under the current version of this standard.				
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Affirmative	Further clarification should be pursued either through a future revision of the standard or a SAR specificall for the last sentence “Devices controlling access into the Electronic Security Perimeter are not exempt.” Suggest removing or replacing with “Devices controlling access into the Electronic Security Perimeter must comply with the Standards, as described in CIP-005 R1.5

Voter	Entity	Segment	Vote	Comment
Response19: Thank you for your comment and suggestion. There is revision work currently being conducted on standards CIP-002 through CIP-009 under Project 2008-06: Cyber Security Order 706. We suggest that your comments be directed to that drafting team.				
Stanley M Jaskot	Entergy Corporation	5	Affirmative	Need a definition of "encrypted tunnel"
Response20: Thank you for your comment. The drafting team acknowledges your suggestion for a definition of “encrypted tunnel” however the scope of our work is limited to interpreting the existing standard. There is revision work currently being conducted on standards CIP-002 through CIP-009 under Project 2008-06: Cyber Security Order 706. We suggest that your comments, including the proposed new NERC *Glossary of Terms Used in Reliability Standards* definition, be directed to that drafting team.				
Peter T Yost	Consolidated Edison Co. of New York	3	Affirmative	Regarding the CIP-005 Interpretation, the following comment is submitted: "Further clarification should be pursued either through a future revision of the standard or a SAR specifically for the last sentence "Devices controlling access into the Electronic Security Perimeter are not exempt." Suggest removing or replacing with "Devices controlling access into the Electronic Security Perimeter must comply with the Standards, as described in CIP-005 R1.5."
Response21: Thank you for your comment and suggestion. There is revision work currently being conducted on standards CIP-002 through CIP-009 under Project 2008-06: Cyber Security Order 706. We suggest that your comments be directed to that drafting team.				
Ronald D. Schellberg	Idaho Power Company	1	Abstain	Interpretation does not aid in the interpretation of the standard.
Response22: Thank you for your comment. 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.				
Jerome Murray	Oregon Public Utility Commission	9	Abstain	Our concern is the lack of clarity around the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links”. Unfortunately, the proposed interpretation provides no meaningful clarity.
Response23: Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The drafting team interprets that either physical or logical data communications links are included and whether their endpoints are access points or not depends on the design and architecture.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Recirculation Ballot Window Open

October 16–26, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Project 2009-12: Interpretation of CIP-005-1 for PacifiCorp

A recirculation ballot window for an interpretation of standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s) Section 4.2.2 and Requirement R1.3 for PacifiCorp is now open **until 8 p.m. EDT on October 26, 2009**.

Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Recirculation Ballot Process

The Standards Committee encourages all members of the ballot pool to review the consideration of comments submitted with the initial ballots. In the recirculation ballot, votes are counted by exception only — if a ballot pool member does not submit a revision to that member's original vote, the vote remains the same as in the first ballot. Members of the ballot pool may:

- Reconsider and change their vote from the first ballot.
- Vote in the second ballot even if they did not vote on the first ballot.
- Take no action if they do not want to change their original vote.

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

PacifiCorp requested clarification on the meaning of "associated" cyber assets referenced in Section 4.2.2, the meaning of "endpoint" in Requirement R1.3, and the relationship of an endpoint and an "access point."

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2009-12_Interpretation_CIP-005-1_PacifiCorp.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Final Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Project 2009-12: Interpretation of CIP-005-1 for PacifiCorp
The recirculation ballot for an interpretation of standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3, for PacifiCorp ended October 26, 2009.

Ballot Results
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 86.29%
Approval: 83.25%

The ballot pool approved the interpretation. Ballot criteria details are listed at the end of the announcement.

Next Steps
The interpretation will be submitted to the NERC Board of Trustees for approval.

Project Background
PacifiCorp requested clarification on the meaning of "associated" cyber assets referenced in Section 4.2.2, the meaning of "endpoint" in Requirement R1.3, and the relationship of an endpoint and an "access point."

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2009-12_Interpretation_CIP-005-1_PacifiCorp.html

Standards Development Process
The *Reliability Standards Development Procedure* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria
Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results

Ballot Name:	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1_rc
Ballot Period:	10/16/2009 - 10/26/2009
Ballot Type:	recirculation
Total # Votes:	214
Total Ballot Pool:	248
Quorum:	**86.29 % The Quorum has been reached**
Weighted Segment Vote:	83.25 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	67	1	34	0.723	13	0.277	9	11
2 - Segment 2.	10	0.7	6	0.6	1	0.1	2	1
3 - Segment 3.	59	1	40	0.833	8	0.167	2	9
4 - Segment 4.	11	1	9	0.9	1	0.1	0	1
5 - Segment 5.	45	1	27	0.73	10	0.27	3	5
6 - Segment 6.	33	1	20	0.741	7	0.259	2	4
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.6	6	0.6	0	0	0	2
9 - Segment 9.	8	0.6	5	0.5	1	0.1	1	1
10 - Segment 10.	7	0.7	7	0.7	0	0	0	0
Totals	**248**	**7.6**	**154**	**6.327**	**41**	**1.273**	**19**	**34**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Avista Corp.	Scott Kinney	Abstain	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Negative	View

1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	E.ON U.S. LLC	Larry Monday		
1	East Kentucky Power Coop.	George S. Carruba		
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Abstain	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Abstain	View
1	ITC Transmission	Elizabeth Howell	Negative	
1	JEA	Ted E Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Kissimmee Utility Authority	Joe B Watson		
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	Rodney Hawkins		
1	Lincoln Electric System	Doug Bantam		
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	National Grid	Manuel Couto		
1	Nebraska Public Power District	Richard L. Koch	Abstain	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Negative	
1	Pacific Gas and Electric Company	Chifong L. Thomas		
1	PacifiCorp	Mark Sampson		
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Affirmative	
1	PP&L, Inc.	Ray Mammarella	Negative	View
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Puget Sound Energy, Inc.	Catherine Koch	Affirmative	
1	Salt River Project	Robert Kondziolka	Negative	View
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SaskPower	Wayne Guttormson	Abstain	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Abstain	
1	Southern California Edison Co.	Dana Cabbell	Negative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Negative	View
1	Tampa Electric Co.	Thomas J. Szelistowski	Abstain	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	View
2	Alberta Electric System Operator	Jason L. Murray	Abstain	
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Abstain	

2	New Brunswick System Operator	Alden Briggs		
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Affirmative	
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana		
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Black Hills Power	Andy Butcher	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	City of Farmington	Linda R. Jacobson		
3	City Public Service of San Antonio	Edwin Les Barrow	Affirmative	
3	Colorado Springs Utilities	Alan Laborwit	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	View
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	East Kentucky Power Coop.	Sally Witt	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W. Pourciau	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory David Woessner		
3	Lakeland Electric	Mace Hunter		
3	Lincoln Electric System	Bruce Merrill	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C Parent	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	Mark Alberter	Negative	View
3	Salt River Project	John T. Underhill	Negative	View
3	San Diego Gas & Electric	Scott Peterson		
3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Negative	View
3	Tampa Electric Co.	Ronald L. Donahey		
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	View
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt		
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	

4	Northern California Power Agency	Fred E. Young	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Calpine Corporation	John Brent Hebert		
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Robert Smith	Negative	View
5	Dynegy	Greg Mason	Negative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	View
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	Kansas City Power & Light Co.	Scott Heidtbrink	Negative	View
5	Lakeland Electric	Thomas J Trickey	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin	Affirmative	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	Michigan Public Power Agency	James R. Nickel	Affirmative	View
5	MidAmerican Energy Co.	Christopher Schneider	Abstain	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp Energy	David Godfrey	Negative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PPL Generation LLC	Mark A. Heimbach	Negative	View
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik		
5	RRI Energy	Thomas J. Bradish	Negative	View
5	Salt River Project	Glen Reeves	Negative	View
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	South California Edison Company	Ahmad Sanati		
5	South Carolina Electric & Gas Co.	Richard Jones	Affirmative	
5	Tampa Electric Co.	Frank L Busot	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Eugene Water & Electric Board	Daniel Mark Bedbury	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Thomas Saitta	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	

6	Louisville Gas and Electric Co.	Daryn Barker	Affirmative	
6	Luminant Energy	Thomas Burke		
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PacifiCorp	Gregory D Maxfield	Negative	
6	Portland General Electric Co.	John Jamieson		
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Negative	View
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Southern California Edison Co.	Marcus V Lotto	Negative	View
6	Tampa Electric Co.	Joann Wehle		
6	Western Area Power Administration - UGP Marketing	John Stonebarger	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Negative	View
8	Edward C Stein	Edward C Stein	Affirmative	
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz		
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
8	Wally Magda	Wally Magda	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	View
9	Public Service Commission of South Carolina	Philip Riley	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Negative	
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	View
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Exhibit D

Roster of the Interpretation Development Team

Request for Interpretation of CIP-005-01 by PacifiCorp Drafting Team

Project 2009-12

	David L. Norton (Chair)	Entergy
	Jackie Collett	Manitoba Hydro
	Jeri Domingo Brewer	U.S. Bureau of Reclamation
	Gerald Freese	American Electric Power
	John Lim	Con Edison
	Robert Mathews	PG&E
	Kevin B. Perry	SPP
NERC Staff	Scott Mix — Manager Infrastructure Security	North American Electric Reliability Corporation
NERC Staff	Harry Tom — Standards Development Coordinator	North American Electric Reliability Corporation