



May 6, 2010

**VIA ELECTRONIC FILING**

Kirsten Walli, Board Secretary  
Ontario Energy Board  
P.O Box 2319  
2300 Yonge Street  
Toronto, Ontario, Canada  
M4P 1E4

Re: *North American Electric Reliability Corporation*

Dear Ms. Walli:

The North American Electric Reliability Corporation (“NERC”) hereby submits this petition seeking approval for an interpretation of Requirement R1.1 in NERC Reliability Standard CIP-006-3 — Cyber Security — Physical Security of Critical Cyber Assets, as set forth in **Exhibit A** to this petition. Upon approval, the standard that includes the interpretation will be referred to as CIP-006-3c.<sup>1</sup>

---

<sup>1</sup> In its submission to the Federal Energy Regulatory Commission (“FERC”), NERC explained that, at the time this interpretation was submitted to NERC, Version 1 of the CIP standards was the version in effect. The request for interpretation was therefore processed referencing CIP-006-1. Since then, CIP-006-2 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 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. NERC noted in its FERC filing that, upon FERC approval of the interpretation, the standard that included the interpretation will be referred to as either CIP-005-2a or CIP-005-3a, depending on which version of the standard is in effect at the time of FERC approval. Thus, if FERC has not approved CIP-005-3 when it approves this interpretation, the interpretation will be referred to as CIP-005-2a until CIP-005-3 is approved by FERC.

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

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-006-3 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1 submitted for approval (**Exhibit A**);
- Reliability Standard CIP-006-3c – Cyber Security – Physical Security of Critical Cyber Assets, that includes the appended interpretation of Requirement R1.1 (**Exhibit B**);
- 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*

---

**BEFORE THE  
ONTARIO ENERGY BOARD  
OF THE PROVINCE OF ONTARIO**

**NORTH AMERICAN ELECTRIC                                     )  
RELIABILITY CORPORATION                                     )**

**PETITION OF THE  
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR  
APPROVAL OF INTERPRETATION TO RELIABILITY STANDARD CIP-006-3  
— CYBER SECURITY — PHYSICAL SECURITY OF CRITICAL CYBER  
ASSETS, REQUIREMENT R1.1**

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

May 6, 2010

---

## TABLE OF CONTENTS

|      |  |   |
|------|--|---|
| I.   | Introduction   | 1 |
| II.  | Notices and Communications   | 2 |
| III. | Background   | 2 |
|      | a. Basis for Approval of Proposed Interpretation   | 2 |
|      | b. Reliability Standards Development Procedure and Interpretation  | 2 |
| IV.  | Reliability Standard CIP-006-3 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1 | 3 |
|      | a. Justification for Approval of Interpretation  | 4 |
|      | b. Summary of the Reliability Standard Development Proceedings   | 6 |
| V.   | Conclusion   | 9 |

Exhibit A — Interpretation of Reliability Standard CIP-006-2 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, Proposed for Approval.

Exhibit B — Reliability Standards CIP-006-3— Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, that includes the appended interpretation.

Exhibit C — Complete Record of Development of the Interpretation for Reliability Standards CIP-006-2c— Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1.

Exhibit D — Roster of the Interpretation Development Team.

## I. INTRODUCTION

The North American Electric Reliability Corporation (“NERC”) hereby requests approval of an interpretation to a requirement of a NERC Reliability Standard:

- CIP-006-3 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1<sup>2</sup>

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-006-3 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, on February 16, 2010. NERC requests approval of the Reliability Standard CIP-006-3c, that includes the appended interpretation and make the standard effective immediately upon approval. **Exhibit A** to this filing sets forth the proposed interpretation. **Exhibit B** contains the CIP-006-3c Reliability Standard that includes the appended interpretation. **Exhibit C** contains the complete development record of the proposed interpretation to CIP-006-3 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1. **Exhibit D** contains a roster of the interpretation development team.

---

<sup>2</sup> In its submission to FERC, NERC explained that, at the time this interpretation was submitted to NERC, Version 1 of the CIP standards was the version in effect. The request for interpretation was therefore processed referencing CIP-006-1. Since then, CIP-006-2 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. NERC noted in its FERC filing that, upon FERC approval of the interpretation, the standard that included the interpretation will be referred to as either CIP-005-2a or CIP-005-3a, depending on which version of the standard is in effect at the time of FERC approval. Thus, if FERC has not approved CIP-005-3 when it approves this interpretation, the interpretation will be referred to as CIP-005-2a until CIP-005-3 is approved by FERC.

NERC filed this interpretation with FERC on April 20, 2010, and is also filing this interpretation with the other 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](mailto: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](mailto:rebecca.michael@nerc.net)  
[holly.hawkins@nerc.net](mailto:holly.hawkins@nerc.net)

## **III. BACKGROUND**

### **a. 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 approval of this interpretation.

### **b. 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 NERC Rules of Procedure as Appendix 3A.<sup>3</sup> Upon request, NERC will assemble a team with the relevant expertise to address the interpretation request and, 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 Procedure*, 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-006-3 — Cyber Security — Physical Security of Critical Cyber Assets Requirement R1.1**

NERC submitted CIP-006-3 on January 21, 2010. This filing includes the proposed Reliability Standard CIP-006-3c that contains the appended interpretation in **Exhibit B**. In Section IV (a), below, NERC discusses the proposed interpretation to the standard, and explains the need for the development of an interpretation to Requirement R1.1 of the CIP-006 Reliability Standard. In this discussion, NERC demonstrates that the interpretation is consistent with the stated reliability goals of the Reliability Standard. Section IV (b) below, describes the stakeholder ballot results and an explanation of how

---

<sup>3</sup> See NERC's *Reliability Standards Development Procedure Version 7*, approved by the NERC Board of Trustees on November 5, 2009, available at [http://www.nerc.com/files/Appendix\\_3A\\_ReliabilityStandardsDevelopmentProcedure\\_02052010.pdf](http://www.nerc.com/files/Appendix_3A_ReliabilityStandardsDevelopmentProcedure_02052010.pdf).

stakeholder comments were considered and addressed by the interpretation development team assembled to provide the interpretation.

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 developed the proposed interpretation.

#### **a. Justification for Approval of Interpretation**

The stated purpose of Reliability Standard CIP-006-3 — Cyber Security — Physical Security of Critical Cyber Assets is to ensure the implementation of a physical security program for the protection of Critical Cyber Assets

Requirement R1 of the standard provides:

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

**R1.1.** All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.<sup>4</sup>

On February 6, 2009, PacifiCorp, with a shared interest from nine other registered entities, submitted a request for formal interpretation of CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1. The focus of the request is whether “alternative measures” must be physical in nature.

---

<sup>4</sup> The requirements in R1 and R1.1 of CIP-006-3 are identical to the R1 and R1.1 requirements in the FERC-approved CIP-006-2 version of the standard.



PacifiCorp requested clarification on several aspects of Requirement R1.1 as outlined in the questions below. Members of the Cyber Security Order No. 706 Standard Authorization Request (“SAR”) Standard Drafting Team were assigned to develop the response to the interpretation request that is presented below:

**Question**

If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access *e.g.* using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?

Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

**Response**

*For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are “physical in nature.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.*

The interpretation is consistent with the stated purpose of the Reliability Standard, which is to ensure that Critical Cyber Assets are protected. As part of a physical security program, the standard requires the creation and maintenance of a Physical Security Plan that addresses protection of Cyber Assets within a Physical Security Perimeter. Where a completely enclosed border cannot be established, the Reliability Standard permits the deployment of alternative measures to control physical access. In this context, the interpretation request discusses connections between multiple Physical Security

Perimeters that reside within a single Electronic Security Perimeter, and the protection of Cyber Assets within it.

The interpretation clarifies that alternative measures to “control” physical access may comprise both physical as well as logical measures. Acceptable alternative non-physical control measures may include, for example, data encryption for protection and circuit monitoring for detection of unauthorized physical access or tampering. The main objective of the Reliability Standard can be achieved through any measure, physical or logical, that succeeds in controlling physical access to the Critical Cyber Asset, providing an equivalent security posture consistent with the intent of the standard and objective of the requirement. The interpretation therefore is consistent with the Reliability Standard’s purpose.

#### **b. Summary of the Reliability Standard Development Proceedings**

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 84.92 percent with a weighted affirmative approval of 79.04 percent. There were 34 negative ballots submitted in the initial ballot, and 20 of those ballots included a comment, which initiated the need for a recirculation ballot.

The recirculation ballot was conducted from December 11, 2009 through December 23, 2009 and achieved a quorum of 90.08 percent with a weighted affirmative approval of 78.77 percent. There were 39 negative ballots submitted in the recirculation ballot, and 22 of those ballots included a comment. Some balloters listed more than one reason for their negative ballot.

As demonstrated in the summary of comments presented below, several commenters noted disagreement with the standard drafting team's interpretation that wiring is a component of a communication network and needs protection. More specifically, the reasons cited for the negative ballots included the following:

- Five balloters did not believe the interpretation fully addressed the issues raised by PacifiCorp. The balloters indicated the response only addressed the ESP wiring external to a PSP and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border.
- Three balloters indicated wiring does not qualify as a Critical Cyber Asset subject to CIP requirements. Some balloters offered opinions of what should be considered Critical Cyber Assets:
  - Critical Cyber Assets are those that are IP addressable (routable) or accessible via hard lines (*i.e.* telephone or modem).
  - Critical Cyber Assets are those components to which the wires are connected, such as patch panels, routers, switches, *etc.*
- Three balloters indicated the response to question 3 is confusing and introduces ambiguity into the standards, stating that a thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.
- Two balloters indicated the question being asked is broader than just the location of the wiring that makes up part of the ESP. One balloter requested more specifics for what constitutes appropriate alternative measures, what is meant by control, and how a logical measure could be equivalent to or better than a physical measure, stating that logical controls will not prevent a cable from being cut.
- Two balloters indicated that Requirement R1.1 requires physical measures and does not reference logical measures. One balloter stated that encryption does not control physical access in any way. Though the balloter indicated support for allowing alternative protective measures, both balloters indicated this interpretation would essentially change the requirement and standard, which is inconsistent with the NERC *Reliability Standards Development Procedure* (*i.e.*, interpretations may not be used to change a requirement or a standard).
- One balloter indicated the interpretation lacked clarity regarding the characteristics of an "endpoint" and what devices are in scope as being associated with "data communication links."
- One balloter suggested the drafting team explain the purpose of a six-wall border and measures for effectiveness, which would allow for an alternative implementation to be measured.

- One balloter requested clarification regarding whether “wiring” is meant as physical wires or a broader concept of communication paths, “including intermediate devices such as repeaters, bridges, frame relay devices, MPLS nodes, etc.” The balloter also requested clarification regarding which elements of security need to be provided (confidentiality, integrity, availability, *etc.*).
- One balloter seemed to indicate support for this interpretation but voted no with a reference to another interpretation. The balloter indicated this interpretation for CIP-006-1 Requirement R1 clarifies the option to use logical controls as alternative measures, which is something the company supported. The balloter explained the posted interpretation of CIP-005-1, Section 4.2.2 and CIP-005-1, Requirement R1.3, did provide the clarity the company sought regarding the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links.”
- One balloter indicated the response introduces a reference to wiring, but the question did not specifically refer to wiring.
- One balloter indicated concern that this interpretation would make compliance at power plants nearly impossible.
- One balloter indicated that the interpretation response inadvertently resulted in expanding the requirements of the standard rather than interpreting the existing requirement. The balloter stated that neither Requirement R1.1 (CIP-006-1) nor Requirement 3 (CIP-002-1) specifically discusses or identifies wiring as a Critical Cyber Asset that would need physical protection within a six-wall barrier.

The standard drafting team responded to comments by explaining that the definition of Cyber Asset in the NERC Glossary includes communication networks, and that the physical media (wiring) is a component of the communication network. Furthermore, the standard drafting team indicated its belief that logical methods are within the spectrum of potential alternative measures for CIP-006 Requirement R1.1.<sup>5</sup>

---

<sup>5</sup> Note that FERC also ordered NERC to include this requirement in those to be considered for Technical Feasibility Exceptions (“TFEs”). See *North American Electric Reliability Corporation*, “Order Approving Technical Feasibility Exception Procedures And Ordering Compliance Filing,” 130 FERC ¶ 61,050 (January 21, 2010).

V. **CONCLUSION**

NERC respectfully requests approval of the interpretation to FERC-approved Reliability Standard CIP-006-3— Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, as set out in **Exhibit A**. NERC requests that this interpretation be made effective immediately upon approval.

Respectfully submitted,

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](mailto:david.cook@nerc.net)

/s/ Holly A. Hawkins  
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](mailto:rebecca.michael@nerc.net)  
[holly.hawkins@nerc.net](mailto:holly.hawkins@nerc.net)

**Exhibit A**

**Interpretation of Reliability Standard CIP-006-2 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1 Proposed for Approval**

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

| Request for an Interpretation of a Reliability Standard  |   |
|--|---|
| <b>Date submitted:</b>   | 02/06/09  |
| Contact information for person requesting the interpretation:  |   |
| <b>Name:</b>   | Daniel Marvin                                   |
| <b>Organization:</b>   | PacifiCorp                                      |
| <b>Telephone:</b>  | 503.813.5375                                    |
| <b>E-mail:</b>   | daniel.marvin@pacificorp.com                    |
| Identify the standard that needs clarification:  |   |
| <b>Standard Number (include version number):</b>   | CIP-006-1.R1.1                                  |
| <b>Standard Title:</b>   | CIP-006-1 --Cyber Security -- Physical Security |
| Identify specifically what needs clarification (If a category is not applicable, please leave it blank):   |   |
| <b>Requirement Number and Text of Requirement:</b>   | CIP-006-1 R1.1                                  |
| <p><b>R1.1</b> Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.</p>   |   |
| <b>Clarification needed:</b>   |   |
| <p>If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?</p> |   |
| <p>Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?</p>   |   |
| 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.

**Other industry entities interested in the clarification requested above are:**

- PacifiCorp
- 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 2009-13: Response to Request for an Interpretation of CIP-006-1 Requirement R1.1 for PacifiCorp**

The following interpretation of CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets was developed by the Cyber Security Order 706 SAR drafting team.

**Requirement Number and Text of Requirement**

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

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

**Question**

If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?

Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

**Response**

For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are “physical in nature.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

## **Exhibit B**

**Reliability Standard CIP-006-3c — Cyber Security — Physical Security of Critical  
Cyber Assets, Requirement R1.1 that includes the Appended Interpretation  
(Clean and Redline)**

## A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets
2. **Number:** CIP-006-3c
3. **Purpose:** Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 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-006-3, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator
    - 4.1.2 Balancing Authority
    - 4.1.3 Interchange Authority
    - 4.1.4 Transmission Service Provider
    - 4.1.5 Transmission Owner
    - 4.1.6 Transmission Operator
    - 4.1.7 Generator Owner
    - 4.1.8 Generator Operator
    - 4.1.9 Load Serving Entity
    - 4.1.10 NERC
    - 4.1.11 Regional Entity
  - 4.2. The following are exempt from Standard CIP-006-3:
    - 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 the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
  - R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
  - R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
  - R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

- R1.4.** Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
- R1.5.** Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
- R1.6.** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
  - R1.6.1.** Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
  - R1.6.2.** Continuous escorted access of visitors within the Physical Security Perimeter.
- R1.7.** Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
- R1.8.** Annual review of the physical security plan.
- R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
  - R2.1.** Be protected from unauthorized physical access.
  - R2.2.** Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
- R3.** Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.
- R4.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
  - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
  - Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
  - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
  - Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
- R5.** Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
  - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.
- R6.** Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
- Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.
  - Video Recording: Electronic capture of video images of sufficient quality to determine identity.
  - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
- R7.** Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.
- R8.** Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:
- R8.1.** Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
  - R8.2.** Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.
  - R8.3.** Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

**C. Measures**

- M1.** The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.
- M2.** The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.
- M5.** The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.
- M6.** The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

- M7.** The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.
- M8.** The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

## **D. Compliance**

### **1. Compliance Monitoring Process**

#### **1.1. Compliance Enforcement Authority**

- 1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- 1.1.2** ERO for Regional Entities.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

#### **1.2. Compliance Monitoring Period and Reset Time Frame**

Not applicable.

#### **1.3. Compliance Monitoring and Enforcement Processes**

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

#### **1.4. Data Retention**

- 1.4.1** The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### **1.5. Additional Compliance Information**

- 1.5.1** The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.
- 1.5.2** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

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

## **E. Regional Variances**

None identified.

**Version History**

| <b>Version</b> | <b>Date</b> | <b>Action</b>   | <b>Change Tracking</b> |
|----------------|-------------|---|------------------------|
| 2              |             | <p>Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Replaced the RRO with RE as a responsible entity.</p> <p>Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager.</p> <p>Revised the wording in R1.2 to identify all “physical” access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2.</p> <p>Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter.</p> <p>The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements.</p> <p>Changed the Compliance Monitor to Compliance Enforcement Authority.</p> |                        |
| 3              |             | <p>Updated version numbers from -2 to -3</p> <p>Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009.</p> <p>In Requirement R7, the term “Responsible Entity” was capitalized.</p>   |                        |
|                | 11/18/2009  | Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7  |                        |
| 3              | 12/16/09    | Approved by NERC Board of Trustees  | Update                 |
| 1a             | 02/12/08    | Added Appendix 1: Interpretation of R1 and Additional Compliance Information Section 1.4.4 as adopted by the Board of Trustees  | Interpretation         |
| 1b             | 08/05/09    | Added Appendix 2: Interpretation of R4 as adopted by the Board of Trustees  | Interpretation         |
| 3c             | 02/16/10    | Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010  | Interpretation         |

## Appendix 1

### Interpretation of Requirement R1.1.

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

**Interpretation:**

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

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

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

**R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.**

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

**1.4. Additional Compliance Information**

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



## Appendix 2

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

### Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, “time of access” mean logging when the person entered the facility or does it mean logging the entry/exit time and “length” of time the person had access to the critical asset?*

### Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term “time of access” refers to the time an authorized individual enters the physical security perimeter.

### Requirement Number and Text of Requirement

- R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:**
- R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.**
  - R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.**
  - R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.**

### Appendix 3

| <b>Requirement Number and Text of Requirement</b>   |
|---|
| <p>R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:</p> <p style="padding-left: 40px;">R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.</p>   |
| <b>Question</b>   |
| <p>If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?</p> <p>Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?</p>   |
| <b>Response</b>   |
| <p>For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are “physical in nature.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p> |

## A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets
2. **Number:** CIP-006-3c
3. **Purpose:** Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 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-006-3, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator
    - 4.1.2 Balancing Authority
    - 4.1.3 Interchange Authority
    - 4.1.4 Transmission Service Provider
    - 4.1.5 Transmission Owner
    - 4.1.6 Transmission Operator
    - 4.1.7 Generator Owner
    - 4.1.8 Generator Operator
    - 4.1.9 Load Serving Entity
    - 4.1.10 NERC
    - 4.1.11 Regional Entity
  - 4.2. The following are exempt from Standard CIP-006-3:
    - 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 the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
  - R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
  - R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
  - R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

- R1.4.** Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
- R1.5.** Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
- R1.6.** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
  - R1.6.1.** Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
  - R1.6.2.** Continuous escorted access of visitors within the Physical Security Perimeter.
- R1.7.** Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
- R1.8.** Annual review of the physical security plan.
- R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
  - R2.1.** Be protected from unauthorized physical access.
  - R2.2.** Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
- R3.** Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.
- R4.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
  - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
  - Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
  - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
  - Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
- R5.** Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
  - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.
- R6.** Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
- Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.
  - Video Recording: Electronic capture of video images of sufficient quality to determine identity.
  - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
- R7.** Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.
- R8.** Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:
- R8.1.** Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
  - R8.2.** Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.
  - R8.3.** Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

### C. Measures

- M1.** The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.
- M2.** The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.
- M5.** The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.
- M6.** The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

- M7.** The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.
- M8.** The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

## **D. Compliance**

### **1. Compliance Monitoring Process**

#### **1.1. Compliance Enforcement Authority**

- 1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- 1.1.2** ERO for Regional Entities.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

#### **1.2. Compliance Monitoring Period and Reset Time Frame**

Not applicable.

#### **1.3. Compliance Monitoring and Enforcement Processes**

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

#### **1.4. Data Retention**

- 1.4.1** The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### **1.5. Additional Compliance Information**

- 1.5.1** The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.
- 1.5.2** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

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

## **E. Regional Variances**

None identified.

**Version History**

| <b>Version</b>     | <b>Date</b>              | <b>Action</b>   | <b>Change Tracking</b>         |
|--------------------|--------------------------|---|--------------------------------|
| 2                  |                          | <p>Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Replaced the RRO with RE as a responsible entity.</p> <p>Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager.</p> <p>Revised the wording in R1.2 to identify all “physical” access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2.</p> <p>Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter.</p> <p>The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements.</p> <p>Changed the Compliance Monitor to Compliance Enforcement Authority.</p> |                                |
| 3                  |                          | <p>Updated version numbers from -2 to -3</p> <p>Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009.</p> <p>In Requirement R7, the term “Responsible Entity” was capitalized.</p>   |                                |
|                    | 11/18/2009               | Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7  |                                |
| 3                  | 12/16/09                 | Approved by NERC Board of Trustees  | Update                         |
| <a href="#">1a</a> | <a href="#">02/12/08</a> | <a href="#">Added Appendix 1: Interpretation of R1 and Additional Compliance Information Section 1.4.4 as adopted by the Board of Trustees</a>  | <a href="#">Interpretation</a> |
| <a href="#">1b</a> | <a href="#">08/05/09</a> | <a href="#">Added Appendix 2: Interpretation of R4 as adopted by the Board of Trustees</a>  | <a href="#">Interpretation</a> |
| <a href="#">3c</a> | <a href="#">02/16/10</a> | <a href="#">Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010</a>  | <a href="#">Interpretation</a> |

## Appendix 1

### Interpretation of Requirement R1.1.

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

**Interpretation:**

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

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

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

**R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.**

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

**1.4. Additional Compliance Information**

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



## Appendix 2

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

### Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, “time of access” mean logging when the person entered the facility or does it mean logging the entry/exit time and “length” of time the person had access to the critical asset?*

### Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term “time of access” refers to the time an authorized individual enters the physical security perimeter.

### Requirement Number and Text of Requirement

- R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:**
- R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.**
  - R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.**
  - R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.**

### Appendix 3

#### Requirement Number and Text of Requirement

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

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

#### Question

If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?

Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

#### Response

For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are “physical in nature.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

**Exhibit C**

**Complete Record of Development of the interpretation for Reliability Standard  
CIP-006-2c — Cyber Security — Physical Security of Critical Cyber Assets,  
Requirement R1.1**

## Project 2009-13 Interpretation of CIP-006-1 R1.1

**Status:**

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

**Summary:**


The request asks to clarify the following: If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

**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-006-1<br><br><a href="#">Interpretation (1)</a><br><br><a href="#">Request for Interpretation (2)</a> | Recirculation Ballot<br><br><a href="#">Info&gt;&gt; (8)</a>  <br><a href="#">Vote&gt;&gt;</a> | 12/11/09 -<br>12/23/09<br>(closed) | <a href="#">Summary&gt;&gt; (9)</a><br><br><a href="#">Full Record&gt;&gt; (10)</a> |   |
|  | Initial Ballot<br><br><a href="#">Info&gt;&gt; (4)</a>  <br><a href="#">Vote&gt;&gt;</a>       | 08/27/09 -<br>09/08/09<br>(closed) | <a href="#">Summary&gt;&gt; (5)</a><br><br><a href="#">Full Record&gt;&gt; (6)</a>  | <a href="#">Consideration of Comments&gt;&gt; (7)</a> |
|  | Pre-ballot Review<br><br><a href="#">Info&gt;&gt; (3)</a>  <br><a href="#">Join&gt;&gt;</a>    | 07/27/09 -<br>08/27/09<br>(closed) |   |   |

To download a file click on the file using your right mouse button, then save it to your computer in a directory of your choice.

|   |   |
|---|---|
| Documents in the PDF format require use of the Adobe Reader® software. Free <a href="#">Adobe Reader®</a> software allows anyone view and print Adobe <a href="#">Portable Document Format (PDF)</a> files. For more information download the <a href="#">Adobe Reader User Guide</a> . |  |
|---|---|

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

| Request for an Interpretation of a Reliability Standard   |   |
|---|---|
| <b>Date submitted:</b>  | 02/06/09  |
| <b>Contact information for person requesting the interpretation:</b>  |   |
| <b>Name:</b>  | Daniel Marvin                                   |
| <b>Organization:</b>  | PacifiCorp                                      |
| <b>Telephone:</b>   | 503.813.5375                                    |
| <b>E-mail:</b>  | daniel.marvin@pacificorp.com                    |
| <b>Identify the standard that needs clarification:</b>  |   |
| <b>Standard Number (include version number):</b>  | CIP-006-1.R1.1                                  |
| <b>Standard Title:</b>  | CIP-006-1 --Cyber Security -- Physical Security |
| <b>Identify specifically what needs clarification</b> (If a category is not applicable, please leave it blank):   |   |
| <b>Requirement Number and Text of Requirement:</b>  | CIP-006-1 R1.1                                  |
| <p><b>R1.1</b> Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.</p>  |   |
| <b>Clarification needed:</b>  |   |
| <p>If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?</p> <p>Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?</p> |   |
| <b>Identify the material impact associated with this interpretation:</b>  |   |

## Request for an Interpretation of a Reliability Standard

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

**Other industry entities interested in the clarification requested above are:**

- PacifiCorp
- 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 2009-13: Response to Request for an Interpretation of CIP-006-1 Requirement R1.1 for PacifiCorp

The following interpretation of CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets was developed by the Cyber Security Order 706 SAR drafting team.

### Requirement Number and Text of Requirement

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

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

### Question

If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?

Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

### Response

For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are “physical in nature.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

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

| Request for an Interpretation of a Reliability Standard  |  |
|--|--|
| Date submitted:  | <a href="#">02/06/09</a>   |
| <b>Contact information for person requesting the interpretation:</b>   |  |
| Name:  | <a href="#">Daniel Marvin</a>  |
| Organization:  | <a href="#">PacifiCorp</a>   |
| Telephone:   | <a href="#">503.813.5375</a>   |
| E-mail:  | <a href="mailto:daniel.marvin@pacificorp.com">daniel.marvin@pacificorp.com</a> |
| <b>Identify the standard that needs clarification:</b>   |  |
| Standard Number (include version number):  | <a href="#">CIP-006-1.R1.1</a>   |
| Standard Title:  | <a href="#">CIP-006-1 --Cyber Security -- Physical Security</a>                |
| <b>Identify specifically what needs clarification</b> (If a category is not applicable, please leave it blank):  |  |
| Requirement Number and Text of Requirement:  | <a href="#">CIP-006-1 R1.1</a>   |
| <p><b>R1.1</b> Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.</p>   |  |
| <b>Clarification needed:</b>   |  |
| <p>If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?</p> |  |
| <p>Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?</p>   |  |
| <b>Identify the material impact associated with this interpretation:</b>   |  |



## Request for an Interpretation of a Reliability Standard

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

**Other industry entities interested in the clarification requested above are:**

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



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 2009-13: Interpretation of CIP-006-1 Requirement R1.1 for PacifiCorp**

An interpretation of standard CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets Requirement R1.1 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-2009-13\\_RFI\\_CIP-006\\_in@nerc.com](mailto:bp-2009-13_RFI_CIP-006_in@nerc.com).

#### **Next Steps**

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

#### **Project Background**

PacifiCorp requested clarification on alternative measures for physical access control.

The request and interpretation can be found on the project page:

[http://www.nerc.com/filez/standards/Project2009-13\\_Interpretation\\_CIP-006-1\\_PacifiCorp.html](http://www.nerc.com/filez/standards/Project2009-13_Interpretation_CIP-006-1_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](mailto:shaun.streeter@nerc.net) or at 609.452.8060.*

## Standards Announcement Initial Ballot Window Open August 27–September 8, 2009

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

### **Project 2009-13: Interpretation of CIP-006-1 Requirement R1.1 for PacifiCorp**

An initial ballot window for an interpretation of standard CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets Requirement R1.1 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 alternative measures for physical access control.

The request and interpretation can be found on the project page:

[http://www.nerc.com/filez/standards/Project2009-13\\_Interpretation\\_CIP-006-1\\_PacifiCorp.html](http://www.nerc.com/filez/standards/Project2009-13_Interpretation_CIP-006-1_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](mailto:shaun.streeter@nerc.net) or at 609.452.8060.*



NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## Standards Announcement Initial Ballot Results

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

### **Project 2009-13: Interpretation of CIP-006-1 Requirement R1.1 for PacifiCorp**

The initial ballot for an interpretation of standard CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets Requirement R1.1 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: 84.92%  
Approval: 79.04%

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 alternative measures for physical access control.

The request and interpretation can be found on the project page:

[http://www.nerc.com/filez/standards/Project2009-13\\_Interpretation\\_CIP-006-1\\_PacifiCorp.html](http://www.nerc.com/filez/standards/Project2009-13_Interpretation_CIP-006-1_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](mailto:shaun.streeter@nerc.net) or at 609.452.8060.*

User Name

Password

Log in

Register

- Ballot Pools
- Current Ballots
- Ballot Results
- Registered Ballot Body
- Proxy Voters

[Home Page](#)

| Ballot Results                |  |
|-------------------------------|--|
| <b>Ballot Name:</b>           | Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1_in |
| <b>Ballot Period:</b>         | 8/27/2009 - 9/8/2009   |
| <b>Ballot Type:</b>           | Initial  |
| <b>Total # Votes:</b>         | 214  |
| <b>Total Ballot Pool:</b>     | 252  |
| <b>Quorum:</b>                | <b>84.92 % The Quorum has been reached</b>                   |
| <b>Weighted Segment Vote:</b> | 79.04 %  |
| <b>Ballot Results:</b>        | <b>The standard will proceed to recirculation ballot.</b>    |

| Summary of Ballot Results |             |                |             |            |              |           |                 |          |           |
|---------------------------|-------------|----------------|-------------|------------|--------------|-----------|-----------------|----------|-----------|
| Segment                   | Ballot Pool | Segment Weight | Affirmative |            | Negative     |           | Abstain # Votes | No Vote  |           |
|                           |             |                | # Votes     | Fraction   | # Votes      | Fraction  |                 |          |           |
| 1 - Segment 1.            |             | 69             | 1           | 48         | 0.873        | 7         | 0.127           | 3        | 11        |
| 2 - Segment 2.            |             | 10             | 0.9         | 6          | 0.6          | 3         | 0.3             | 0        | 1         |
| 3 - Segment 3.            |             | 60             | 1           | 44         | 0.898        | 5         | 0.102           | 1        | 10        |
| 4 - Segment 4.            |             | 11             | 1           | 7          | 0.7          | 3         | 0.3             | 0        | 1         |
| 5 - Segment 5.            |             | 47             | 1           | 33         | 0.846        | 6         | 0.154           | 2        | 6         |
| 6 - Segment 6.            |             | 33             | 1           | 20         | 0.769        | 6         | 0.231           | 1        | 6         |
| 7 - Segment 7.            |             | 0              | 0           | 0          | 0            | 0         | 0               | 0        | 0         |
| 8 - Segment 8.            |             | 8              | 0.6         | 3          | 0.3          | 3         | 0.3             | 0        | 2         |
| 9 - Segment 9.            |             | 8              | 0.6         | 6          | 0.6          | 0         | 0               | 1        | 1         |
| 10 - Segment 10.          |             | 6              | 0.6         | 5          | 0.5          | 1         | 0.1             | 0        | 0         |
| <b>Totals</b>             |             | <b>252</b>     | <b>7.7</b>  | <b>172</b> | <b>6.086</b> | <b>34</b> | <b>1.614</b>    | <b>8</b> | <b>38</b> |

| 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      | Affirmative |                      |
| 1                              | BC Transmission Corporation        | Gordon Rawlings   | Negative    | <a href="#">View</a> |
| 1                              | Black Hills Corp                   | Eric Egge         | Affirmative |                      |
| 1                              | Bonneville Power Administration    | Donald S. Watkins | Affirmative |                      |

|   |   |                              |             |                      |
|---|---|------------------------------|-------------|----------------------|
| 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              | Affirmative |                      |
| 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              | Negative    | <a href="#">View</a> |
| 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         | Affirmative |                      |
| 1 | ITC Transmission                                | Elizabeth Howell             | Affirmative |                      |
| 1 | JEA   | Ted E. Hobson                | Negative    |                      |
| 1 | Kansas City Power & Light Co.                   | Michael Gammon               | Negative    | <a href="#">View</a> |
| 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 | Long Island Power Authority                     | Jonathan Appelbaum           | Negative    | <a href="#">View</a> |
| 1 | Manitoba Hydro                                  | Michelle Rheault             | Affirmative |                      |
| 1 | MidAmerican Energy Co.                          | Terry Harbour                | Affirmative |                      |
| 1 | National Grid                                   | Manuel Couto                 | Affirmative |                      |
| 1 | Nebraska Public Power District                  | Richard L. Koch              | Abstain     |                      |
| 1 | New York Power Authority                        | Ralph Ruffano                | 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              | Negative    |                      |
| 1 | Ohio Valley Electric Corp.                      | Robert Matthey               | Affirmative |                      |
| 1 | Oklahoma Gas and Electric Co.                   | Marvin E VanBebber           | Affirmative |                      |
| 1 | Oncor Electric Delivery                         | Charles W. Jenkins           | Affirmative |                      |
| 1 | Orange and Rockland Utilities, Inc.             | Edward Bedder                | Affirmative |                      |
| 1 | Otter Tail Power Company                        | Lawrence R. Larson           | Affirmative |                      |
| 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               | Affirmative |                      |
| 1 | Progress Energy Carolinas                       | Sammy Roberts                | Affirmative |                      |
| 1 | Public Service Electric and Gas Co.             | Kenneth D. Brown             | Affirmative |                      |
| 1 | Puget Sound Energy, Inc.                        | Catherine Koch               |             |                      |
| 1 | Salt River Project                              | Robert Kondziolka            | Affirmative |                      |
| 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                | Affirmative |                      |
| 1 | Southern California Edison Co.                  | Dana Cabbell                 | Affirmative |                      |
| 1 | Southern Company Services, Inc.                 | Horace Stephen Williamson    | Affirmative |                      |
| 1 | Southwest Transmission Cooperative, Inc.        | James L. Jones               | Affirmative |                      |
| 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            | Affirmative |                      |
| 2 | Alberta Electric System Operator                | Jason L. Murray              | Negative    | <a href="#">View</a> |
| 2 | BC Transmission Corporation                     | Faramarz Amjadi              | Negative    | <a href="#">View</a> |
| 2 | California ISO                                  | Greg Tillitson               | Affirmative |                      |
| 2 | Electric Reliability Council of Texas, Inc.     | Chuck B Manning              | Affirmative |                      |
| 2 | Independent Electricity System Operator         | Kim Warren                   | Negative    | <a href="#">View</a> |

|   |   |                         |             |                      |
|---|---|-------------------------|-------------|----------------------|
| 2 | ISO New England, Inc.                         | Kathleen Goodman        | Affirmative |                      |
| 2 | Midwest ISO, Inc.                             | Terry Bilke             | Affirmative |                      |
| 2 | New Brunswick System Operator                 | Alden Briggs            |             |                      |
| 2 | PJM Interconnection, L.L.C.                   | Tom Bowe                | Affirmative |                      |
| 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         | Affirmative |                      |
| 3 | Central Lincoln PUD                           | Steve Alexanderson      |             |                      |
| 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 |                      |
| 3 | Consumers Energy                              | David A. Lapinski       | Affirmative |                      |
| 3 | Cowlitz County PUD                            | Russell A Noble         | Affirmative |                      |
| 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          | Affirmative |                      |
| 3 | East Kentucky Power Coop.                     | Sally Witt              | Affirmative |                      |
| 3 | Entergy Services, Inc.                        | Matt Wolf               | Affirmative |                      |
| 3 | FirstEnergy Solutions                         | Joanne Kathleen Borrell | Negative    | <a href="#">View</a> |
| 3 | Florida Power Corporation                     | Lee Schuster            | Affirmative |                      |
| 3 | Georgia Power Company                         | Leslie Sibert           | Affirmative |                      |
| 3 | Georgia System Operations Corporation         | Edward W Pourciau       | Negative    |                      |
| 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    | <a href="#">View</a> |
| 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         | Negative    |                      |
| 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         | Affirmative |                      |
| 3 | Public Utility District No. 2 of Grant County | Greg Lange              | Affirmative |                      |
| 3 | Sacramento Municipal Utility District         | Mark Alberter           | Affirmative |                      |
| 3 | Salt River Project                            | John T. Underhill       | Affirmative |                      |
| 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         | Negative    | <a href="#">View</a> |
| 3 | Southern California Edison Co.                | David Schiada           | Affirmative |                      |
| 3 | Tampa Electric Co.                            | Ronald L. Donahey       |             |                      |
| 3 | Wisconsin Electric Power Marketing            | James R. Keller         | Affirmative |                      |
| 3 | Xcel Energy, Inc.                             | Michael Ibold           | Affirmative |                      |
| 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           | Negative    |                      |
| 4 | Northern California Power Agency                   | Fred E. Young         | Affirmative |                      |
| 4 | Ohio Edison Company                                | Douglas Hohlbaugh     | Negative    | <a href="#">View</a> |
| 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     | Negative    |                      |
| 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       | Affirmative |                      |
| 5 | Bonneville Power Administration                    | Francis J. Halpin     | Affirmative |                      |
| 5 | Calpine Corporation                                | John Brent Hebert     |             |                      |
| 5 | City of Tallahassee                                | Alan Gale             | Negative    | <a href="#">View</a> |
| 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          | Affirmative |                      |
| 5 | Dynegy   | Greg Mason            | Affirmative |                      |
| 5 | Entergy Corporation                                | Stanley M Jaskot      | Affirmative |                      |
| 5 | Exelon Nuclear                                     | Michael Korchynsky    | Affirmative |                      |
| 5 | FirstEnergy Solutions                              | Kenneth Dresner       | Negative    | <a href="#">View</a> |
| 5 | Great River Energy                                 | Cynthia E Sulzer      | Affirmative |                      |
| 5 | JEA  | Donald Gilbert        | Affirmative |                      |
| 5 | Kansas City Power & Light Co.                      | Scott Heidtbrink      | Negative    |                      |
| 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           | Abstain     |                      |
| 5 | Michigan Public Power Agency                       | James R. Nickel       | Negative    | <a href="#">View</a> |
| 5 | MidAmerican Energy Co.                             | Christopher Schneider | Abstain     |                      |
| 5 | New York Power Authority                           | Gerald Mannarino      | Affirmative |                      |
| 5 | Northern Indiana Public Service Co.                | Michael K Wilkerson   | Negative    |                      |
| 5 | Northern States Power Co.                          | Liam Noailles         | Affirmative |                      |
| 5 | Orlando Utilities Commission                       | Richard Kinas         |             |                      |
| 5 | Pacific Gas and Electric Company                   | Richard J. Padilla    |             |                      |
| 5 | PacifiCorp Energy                                  | David Godfrey         | Affirmative |                      |
| 5 | Portland General Electric Co.                      | Gary L Tingley        | Affirmative |                      |
| 5 | PPL Generation LLC                                 | Mark A. Heimbach      | Affirmative |                      |
| 5 | Progress Energy Carolinas                          | Wayne Lewis           | Affirmative |                      |
| 5 | PSEG Power LLC                                     | Thomas Piascik        |             |                      |
| 5 | RRI Energy   | Thomas J. Bradish     | Affirmative |                      |
| 5 | Salt River Project                                 | Glen Reeves           | Affirmative |                      |
| 5 | Seattle City Light                                 | Michael J. Haynes     | Affirmative |                      |
| 5 | South California Edison Company                    | Ahmad Sanati          |             |                      |
| 5 | South Carolina Electric & Gas Co.                  | Richard Jones         | Negative    | <a href="#">View</a> |
| 5 | Tampa Electric Co.                                 | Frank L Busot         | Affirmative |                      |
| 5 | Tenaska, Inc.                                      | Scott M. Helyer       | Affirmative |                      |
| 5 | TransAlta Centralia Generation, LLC                | Joanna Luong-Tran     | Affirmative |                      |
| 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    | Affirmative |                      |
| 6 | Consolidated Edison Co. of New York                | Nickesha P Carrol     | Affirmative |                      |
| 6 | Constellation Energy Commodities Group             | Chris Lyons           | Negative    |                      |
| 6 | Dominion Resources, Inc.                           | Louis S Slade         | Affirmative |                      |
| 6 | Duke Energy Carolina                               | Walter Yeager         | Affirmative |                      |
| 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  | Negative    | <a href="#">View</a> |
| 6  | Great River Energy   | Donna Stephenson     | Affirmative |                      |
| 6  | Kansas City Power & Light Co.                                | Thomas Saitta        | Negative    | <a href="#">View</a> |
| 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        | Abstain     |                      |
| 6  | New York Power Authority                                     | Thomas Papadopoulos  | Affirmative |                      |
| 6  | Northern Indiana Public Service Co.                          | Joseph O'Brien       | Negative    |                      |
| 6  | PacifiCorp   | Gregory D Maxfield   | Negative    | <a href="#">View</a> |
| 6  | Portland General Electric Co.                                | John Jamieson        |             |                      |
| 6  | Progress Energy  | James Eckelkamp      | Affirmative |                      |
| 6  | PSEG Energy Resources & Trade LLC                            | James D. Hebson      | Affirmative |                      |
| 6  | Public Utility District No. 1 of Chelan County               | Hugh A. Owen         | Affirmative |                      |
| 6  | RRI Energy   | Trent Carlson        | Negative    | <a href="#">View</a> |
| 6  | Salt River Project   | Mike Hummel          |             |                      |
| 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       | Affirmative |                      |
| 6  | Tampa Electric Co.   | Joann Wehle          |             |                      |
| 6  | Western Area Power Administration - UGP Marketing            | John Stonebarger     | Affirmative |                      |
| 6  | Xcel Energy, Inc.  | David F. Lemmons     | Affirmative |                      |
| 8  | Edward C Stein   | Edward C Stein       | Negative    |                      |
| 8  | James A Maenner  | James A Maenner      | Affirmative |                      |
| 8  | JDRJC Associates   | Jim D. Cyrulewski    | Affirmative |                      |
| 8  | Network & Security Technologies                              | Nicholas Lauriat     | Negative    |                      |
| 8  | Power Energy Group LLC                                       | Peggy Abbadini       |             |                      |
| 8  | Roger C Zaklukiewicz   | Roger C Zaklukiewicz |             |                      |
| 8  | Volkman Consulting, Inc.                                     | Terry Volkman        | Negative    |                      |
| 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     |                      |
| 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         | Affirmative |                      |
| 10 | Electric Reliability Council of Texas, Inc.                  | Kent Saathoff        | Affirmative |                      |
| 10 | Midwest Reliability Organization                             | Dan R Schoenecker    | Affirmative |                      |
| 10 | Northeast Power Coordinating Council, Inc.                   | Guy V. Zito          | Affirmative |                      |
| 10 | ReliabilityFirst Corporation                                 | Jacque Smith         | Affirmative |                      |
| 10 | SERC Reliability Corporation                                 | Carter B Edge        | Affirmative |                      |
| 10 | Western Electricity Coordinating Council                     | Louise McCarren      | Negative    | <a href="#">View</a> |

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](#)



**Project 2009-13: Interpretation of CIP-006-1 for PacifiCorp  
Consideration of Comments on Initial Ballot (conducted August 27–September 8, 2009)**

**Summary Consideration:** Of the negative ballots with comments, the majority noted disagreement with the drafting team’s interpretation that wiring is a component of a communication network and needs protection. The drafting team explained that the definition of Cyber Assets in the NERC Glossary of Terms Used in Reliability Standards (Glossary) includes communication networks, and the physical media (wiring) is a component of the communication network.

A minority of comments expressed disagreement with the interpretation that alternate measures include logical methods. The drafting team believes logical methods to be within the spectrum of potential alternate measures for CIP-006-1.

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.<sup>1</sup>

| Voter   | Entity                      | Segment | Vote     | Comment  |
|---|-----------------------------|---------|----------|--|
| Gordon Rawlings   | BC Transmission Corporation | 1       | Negative | BCTC’s interpretation, through reading the requirements, is that cyber assets are those that are IP addressable (routable) or accessible via hard lines (i.e. telephone or modem); wiring is neither.  |
| Faramarz Amjadi   | BC Transmission Corporation | 2       | Negative | BCTC’s interpretation, through reading the requirements, is that cyber assets are those that are IP addressable (routable) or accessible via hard lines (i.e. telephone or modem); wiring is neither.  |
| <p><b>Response1:</b> The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an Electronic Security Perimeter (ESP), but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.</p> |                             |         |          |  |
| Robert Martinko   | FirstEnergy Energy Delivery | 1       | Negative | FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised." |

<sup>1</sup> The appeals process is in the Reliability Standards Development Procedure: [http://www.nerc.com/files/RSDP\\_V6\\_1\\_12Mar07.pdf](http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf).

| Voter                   | Entity                | Segment | Vote     | Comment  |
|-------------------------|-----------------------|---------|----------|--|
| Joanne Kathleen Borrell | FirstEnergy Solutions | 3       | Negative | FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised." |
| Kenneth Dresner         | FirstEnergy Solutions | 5       | Negative | FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised." |
| Mark S Travaglianti     | FirstEnergy Solutions | 6       | Negative | FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised." |
| Douglas Hohlbaugh       | Ohio Edison Company   | 4       | Negative | FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised." |

**Response2:** The drafting team interprets "alternative measures" for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. The requester describes their topology as such therefore the drafting team addressed the issue as stated.

| Voter   | Entity                       | Segment | Vote     | Comment   |
|---|------------------------------|---------|----------|---|
| <p>CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. For ESP wiring that is external to the PSP: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or monitoring to detect unauthorized access or physical tampering.</p> |                              |         |          |   |
| James R. Nickel   | Michigan Public Power Agency | 5       | Negative | MPPA does not believe the intent of R1.1 was to classify wiring as a Cyber Asset subject to the CIP requirements. The term "Cyber Asset" refers to those components to which the wires are connected, such as patch panels, routers, switches etc. MPPA is not arguing that the wiring is irrelevant or unimportant, but contends that it should be handled separately from the existing CIP Standards.   |
| <p><b>Response3:</b> The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.</p>   |                              |         |          |   |
| Gregory D Maxfield  | PacifiCorp                   | 6       | Negative | <p>Regarding PacifiCorp’s requested interpretation of CIP006.R1.1: Our primary concern was commentary from some industry participants who took the view that the phrase “..to control physical access” as used in CIP006.R1.1 represented a requirement for a control that would literally prevent physical access. This viewpoint was not a consensus opinion, but if left unchecked might percolate into the auditor ranks and represent a compliance risk to entities needing to use logical controls as an “alternative measure”. Hence, we took the proactive action of requesting an interpretation from the drafting team. Entities should support this interpretation as it is simply a clarification that entities have the option to use logical controls as alternative measures for CIP006.R1.1.</p> <p>Regarding the posted interpretation of CIP005.4.2.2 and CIP005R1.3: Our 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. We recommend that entities not support this provided interpretation.</p> |
| <p><b>Response4:</b> Thank you for your comment. The drafting team agrees with your position that controlling physical access may encompass both logical and physical measures.</p> <p>In regard your comment on endpoints, the drafting team refers you to the response to comments for Project 2009-12: Interpretation of CIP-005-1 – Cyber Security – Electronic Security Perimeters for PacifiCorp.</p>   |                              |         |          |   |
| Trent Carlson   | RRI Energy                   | 6       | Negative | RRI Energy votes negative in support of PacifiCorp's position. 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.  |

| Voter   | Entity                                   | Segment | Vote     | Comment   |
|---|--|---------|----------|---|
| <p><b>Response5:</b> In regard your comment on endpoints, the drafting team refers you to the response to comments for Project 2009-12: Interpretation of CIP-005-1 – Cyber Security – Electronic Security Perimeters for PacifiCorp.</p>   |  |         |          |   |
| Jonathan Appelbaum  | Long Island Power Authority              | 1       | Negative | The interpretaion team needs to explain what the purpose of a six wall border is and measures for effectiveness. Then the effectiveness of an alternative implemetaion to a six wall border can be measured. For example, is the purpose of a the border to encourage persons to enter thru monitored access points, or is it hardened protection? Once measures are provided then logical controls and alternative methods can be evaluated for effectiveness by the entities.   |
| <p><b>Response6:</b> The drafting team provided an interpretation for the issue requested and does not have the latitude to go beyond what is requested.</p>  |  |         |          |   |
| Louise McCarren   | Western Electricity Coordinating Council | 10      | Negative | The interpretation introduces the option of logical controls where a six-wall border cannot be established. This removes some uncertainty surrounding the language of R1.1. However, a negative vote is being cast for the following reason. Clarification should be provided as to whether the term "wiring" is intended to be exclusive literally to physical wires, or more expansively to communication paths, including intermediate devices such as repeaters, bridges, frame relay devices, MPLS nodes, etc. Clarification should be provided with respect to the particular elements of security which need to be provided (i.e. confidentiality, integrity, availability). If additional clarity is provided we would support this interpretation. |
| <p><b>Response7:</b> The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.</p>   |  |         |          |   |
| Hubert C. Young   | South Carolina Electric & Gas Co.        | 3       | Negative | The question being asked is broader than just the location of the wiring that makes up part of the ESP. The interpretation should address the questions of 1) what constitutes appropriate "alternative measures" if a physical six-wall boundary cannot be established? (motion detectors, video cameras, others) and 2) what is meant by "control"? Also, how can a logical measure be equivalent or better than a physical measure? After all, no matter how encrypted the connection or how well the circuit is monitored via a security system, couldn't someone just cut the cable?   |
| <p><b>Response8:</b> CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p> |  |         |          |   |

| Voter   | Entity                            | Segment | Vote     | Comment   |
|---|-----------------------------------|---------|----------|---|
| Richard Jones   | South Carolina Electric & Gas Co. | 5       | Negative | The question being asked is broader than just the location of the wiring that makes up part of the ESP. The interpretation should address the questions of: 1) What constitutes appropriate "alternative measures" if a physical six-wall boundary cannot be established? (motion detectors, video cameras, others), and 2) What is meant by "control"? In addition, how can a logical measure be equivalent to or better than a physical measure? No matter how encrypted the connection or how well the circuit is monitored via a security system it doesn't stop someone from physically cutting a cable. |
| <p><b>Response9:</b> CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p>   |                                   |         |          |   |
| Michael Gammon  | Kansas City Power & Light Co.     | 1       | Negative | The response to question 3 is confusing and introduces ambiguity into the standards. A thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.  |
| Charles Locke   | Kansas City Power & Light Co.     | 3       | Negative | The response to question 3 is confusing and introduces ambiguity into the standards. A thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.  |
| Thomas Saitta   | Kansas City Power & Light Co.     | 6       | Negative | The response to question 3 is confusing and introduces ambiguity into the standards. A thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.  |
| <p><b>Response10:</b> In regard your comment on endpoints, the drafting team refers you to the response to comments for Project 2009-12: Interpretation of CIP-005-1 – Cyber Security – Electronic Security Perimeters for PacifiCorp.</p>  |                                   |         |          |   |
| Jason L. Murray   | Alberta Electric System Operator  | 2       | Negative | This interpretation would change the standard by allowing the use of safeguards that cannot control physical access, as required by the standard. An interpretation cannot be used to change a standard, and this interpretation would have that effect.  |
| <p><b>Response11:</b> The RFI response drafting team interprets "alternative measures" for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection.</p> <p>CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p> |                                   |         |          |   |

| Voter      | Entity                                  | Segment | Vote     | Comment   |
|------------|---|---------|----------|---|
| Kim Warren | Independent Electricity System Operator | 2       | Negative | While CIP-006-1, Requirement R1.1 clearly requires physical measures, it does not reference logical measures. Thus, our view is that this interpretation effectively alters the requirement, rather than interprets it, with the words "physical or logical" and "Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering." Although we believe the standard should be revised to allow alternative protective measures, doing so within the context of an interpretation is inconsistent with the Reliability Standards Development Procedure. We are therefore of the view that the interpretation needs more work. |

**Response12:** The RFI response drafting team interprets "alternative measures" for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection.

CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

|           |                     |   |          |  |
|-----------|---------------------|---|----------|--|
| Alan Gale | City of Tallahassee | 5 | Negative | While we agree that "alternate logical control measures" should be allowed, we feel the interpretation is still forcing the "wiring" of a "communication network" into the list of what is a Cyber Asset". This we vehemently disagree with. |
|-----------|---------------------|---|----------|--|

**Response13:** The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.





NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## Standards Announcement

### Recirculation Ballot Window Open

December 11-23, 2009

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

#### **Project 2009-13: Interpretation of CIP-006-1 for PacifiCorp**

A recirculation ballot window for an interpretation of standard CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets Requirement R1.1 for PacifiCorp is now open **until 8 p.m. EST on December 23, 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 alternative measures for physical access control.

The request and interpretation can be found on the project page:

[http://www.nerc.com/filez/standards/Project2009-13\\_Interpretation\\_CIP-006-1\\_PacifiCorp.html](http://www.nerc.com/filez/standards/Project2009-13_Interpretation_CIP-006-1_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](mailto:shaun.streeter@nerc.net) or at 609.452.8060.*



NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## Standards Announcement

### Final Ballot Results

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

#### **Project 2009-13: Interpretation of CIP-006-1 for PacifiCorp**

The recirculation ballot for an interpretation of standard CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, for PacifiCorp ended December 23, 2009.

#### **Ballot Results**

Voting statistics are listed below, and the [Ballot Results](#) Web page provides a link to the detailed results:

Quorum: 90.08%  
Approval: 78.77%

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 alternative measures for physical access control.

The request and interpretation can be found on the project page:

[http://www.nerc.com/filez/standards/Project2009-13 Interpretation CIP-006-1 PacifiCorp.html](http://www.nerc.com/filez/standards/Project2009-13%20Interpretation%20CIP-006-1%20PacifiCorp.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](mailto:shaun.streeter@nerc.net) or at 609.452.8060.*

User Name

Password

Log in

Register

- Ballot Pools
- Current Ballots
- Ballot Results
- Registered Ballot Body
- Proxy Voters

[Home Page](#)

| Ballot Results                |  |
|-------------------------------|--|
| <b>Ballot Name:</b>           | Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1_rc |
| <b>Ballot Period:</b>         | 12/11/2009 - 12/23/2009                                      |
| <b>Ballot Type:</b>           | recirculation  |
| <b>Total # Votes:</b>         | 227  |
| <b>Total Ballot Pool:</b>     | 252  |
| <b>Quorum:</b>                | <b>90.08 % The Quorum has been reached</b>                   |
| <b>Weighted Segment Vote:</b> | 78.77 %  |
| <b>Ballot Results:</b>        | <b>The Standard has Passed</b>                               |

| Summary of Ballot Results |             |                |             |              |           |              |                 |           |  |
|---------------------------|-------------|----------------|-------------|--------------|-----------|--------------|-----------------|-----------|--|
| Segment                   | Ballot Pool | Segment Weight | Affirmative |              | Negative  |              | Abstain # Votes | No Vote   |  |
|                           |             |                | # Votes     | Fraction     | # Votes   | Fraction     |                 |           |  |
| 1 - Segment 1.            | 69          | 1              | 49          | 0.845        | 9         | 0.155        | 4               | 7         |  |
| 2 - Segment 2.            | 10          | 1              | 7           | 0.7          | 3         | 0.3          | 0               | 0         |  |
| 3 - Segment 3.            | 60          | 1              | 47          | 0.87         | 7         | 0.13         | 1               | 5         |  |
| 4 - Segment 4.            | 11          | 1              | 7           | 0.7          | 3         | 0.3          | 0               | 1         |  |
| 5 - Segment 5.            | 47          | 1              | 32          | 0.8          | 8         | 0.2          | 3               | 4         |  |
| 6 - Segment 6.            | 33          | 1              | 21          | 0.808        | 5         | 0.192        | 1               | 6         |  |
| 7 - Segment 7.            | 0           | 0              | 0           | 0            | 0         | 0            | 0               | 0         |  |
| 8 - Segment 8.            | 8           | 0.7            | 4           | 0.4          | 3         | 0.3          | 0               | 1         |  |
| 9 - Segment 9.            | 8           | 0.6            | 6           | 0.6          | 0         | 0            | 1               | 1         |  |
| 10 - Segment 10.          | 6           | 0.6            | 5           | 0.5          | 1         | 0.1          | 0               | 0         |  |
| <b>Totals</b>             | <b>252</b>  | <b>7.9</b>     | <b>178</b>  | <b>6.223</b> | <b>39</b> | <b>1.677</b> | <b>10</b>       | <b>25</b> |  |

| 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      | Negative    | <a href="#">View</a> |
| 1                              | Avista Corp.                       | Scott Kinney      | Affirmative |                      |
| 1                              | BC Transmission Corporation        | Gordon Rawlings   | Affirmative | <a href="#">View</a> |
| 1                              | Black Hills Corp                   | Eric Egge         | Affirmative |                      |
| 1                              | Bonneville Power Administration    | Donald S. Watkins | Affirmative |                      |

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

|   |   |                         |             |                      |
|---|---|-------------------------|-------------|----------------------|
| 2 | ISO New England, Inc.                         | Kathleen Goodman        | Affirmative |                      |
| 2 | Midwest ISO, Inc.                             | Terry Bilke             | Affirmative |                      |
| 2 | New Brunswick System Operator                 | Alden Briggs            | Affirmative |                      |
| 2 | PJM Interconnection, L.L.C.                   | Tom Bowe                | Affirmative |                      |
| 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         | Affirmative |                      |
| 3 | Central Lincoln PUD                           | Steve Alexanderson      | Affirmative |                      |
| 3 | City of Farmington                            | Linda R. Jacobson       | Affirmative |                      |
| 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 |                      |
| 3 | Consumers Energy                              | David A. Lapinski       | Negative    |                      |
| 3 | Cowlitz County PUD                            | Russell A Noble         | Affirmative |                      |
| 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          | Affirmative |                      |
| 3 | East Kentucky Power Coop.                     | Sally Witt              | Affirmative |                      |
| 3 | Entergy Services, Inc.                        | Matt Wolf               | Affirmative |                      |
| 3 | FirstEnergy Solutions                         | Joanne Kathleen Borrell | Negative    | <a href="#">View</a> |
| 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           | Affirmative |                      |
| 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             | Affirmative |                      |
| 3 | Kansas City Power & Light Co.                 | Charles Locke           | Negative    | <a href="#">View</a> |
| 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         | Negative    |                      |
| 3 | Orlando Utilities Commission                  | Ballard Keith Muters    | Affirmative |                      |
| 3 | PacifiCorp                                    | John Apperson           | Negative    |                      |
| 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         | Affirmative |                      |
| 3 | Public Utility District No. 2 of Grant County | Greg Lange              | Affirmative |                      |
| 3 | Sacramento Municipal Utility District         | Mark Alberter           | Affirmative |                      |
| 3 | Salt River Project                            | John T. Underhill       | Affirmative |                      |
| 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         | Negative    | <a href="#">View</a> |
| 3 | Southern California Edison Co.                | David Schiada           | Affirmative |                      |
| 3 | Tampa Electric Co.                            | Ronald L. Donahey       |             |                      |
| 3 | Wisconsin Electric Power Marketing            | James R. Keller         | Negative    |                      |
| 3 | Xcel Energy, Inc.                             | Michael Ibold           | Affirmative |                      |
| 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         | Affirmative |                      |
| 4 | Ohio Edison Company                                | Douglas Hohlbaugh     | Negative    | <a href="#">View</a> |
| 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      | Negative    |                      |
| 4 | Wisconsin Energy Corp.                             | Anthony Jankowski     | Negative    |                      |
| 5 | AEP Service Corp.                                  | Brock Ondayko         | Affirmative |                      |
| 5 | Amerenue   | Sam Dwyer             | Affirmative |                      |
| 5 | Avista Corp.                                       | Edward F. Groce       | Affirmative |                      |
| 5 | Bonneville Power Administration                    | Francis J. Halpin     | Affirmative |                      |
| 5 | Calpine Corporation                                | John B. Hebert        |             |                      |
| 5 | City of Tallahassee                                | Alan Gale             | Negative    | <a href="#">View</a> |
| 5 | Colmac Clarion/Piney Creek LP                      | Harvie D. Beavers     | Affirmative |                      |
| 5 | Consumers Energy                                   | James B Lewis         | Negative    | <a href="#">View</a> |
| 5 | Detroit Edison Company                             | Ronald W. Bauer       | Affirmative |                      |
| 5 | Dominion Resources, Inc.                           | Mike Garton           | Affirmative |                      |
| 5 | Duke Energy  | Robert Smith          | Affirmative |                      |
| 5 | Dynegy   | Greg Mason            | Affirmative |                      |
| 5 | Entergy Corporation                                | Stanley M Jaskot      | Affirmative |                      |
| 5 | Exelon Nuclear                                     | Michael Korchynsky    | Affirmative |                      |
| 5 | FirstEnergy Solutions                              | Kenneth Dresner       | Negative    | <a href="#">View</a> |
| 5 | Great River Energy                                 | Cynthia E Sulzer      | Affirmative |                      |
| 5 | JEA  | Donald Gilbert        | Affirmative |                      |
| 5 | Kansas City Power & Light Co.                      | Scott Heidtbrink      | Negative    |                      |
| 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           | Abstain     |                      |
| 5 | Michigan Public Power Agency                       | James R. Nickel       | Negative    | <a href="#">View</a> |
| 5 | MidAmerican Energy Co.                             | Christopher Schneider | Abstain     |                      |
| 5 | New York Power Authority                           | Gerald Mannarino      | Affirmative |                      |
| 5 | Northern Indiana Public Service Co.                | Michael K Wilkerson   | Negative    |                      |
| 5 | Northern States Power Co.                          | Liam Noailles         | Affirmative |                      |
| 5 | Orlando Utilities Commission                       | Richard Kinan         | Affirmative |                      |
| 5 | Pacific Gas and Electric Company                   | Richard J. Padilla    |             |                      |
| 5 | PacifiCorp Energy                                  | David Godfrey         | Affirmative |                      |
| 5 | Portland General Electric Co.                      | Gary L Tingley        | Affirmative |                      |
| 5 | PPL Generation LLC                                 | Mark A. Heimbach      | Affirmative |                      |
| 5 | Progress Energy Carolinas                          | Wayne Lewis           | Affirmative |                      |
| 5 | PSEG Power LLC                                     | Thomas Piascik        |             |                      |
| 5 | RRI Energy   | Thomas J. Bradish     | Affirmative |                      |
| 5 | Salt River Project                                 | Glen Reeves           | Affirmative |                      |
| 5 | Seattle City Light                                 | Michael J. Haynes     | Affirmative |                      |
| 5 | South California Edison Company                    | Ahmad Sanati          |             |                      |
| 5 | South Carolina Electric & Gas Co.                  | Richard Jones         | Negative    | <a href="#">View</a> |
| 5 | Tampa Electric Co.                                 | Frank L Busot         | Affirmative |                      |
| 5 | Tenaska, Inc.                                      | Scott M. Helyer       | Abstain     |                      |
| 5 | TransAlta Centralia Generation, LLC                | Joanna Luong-Tran     | Affirmative |                      |
| 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            | Negative    |                      |
| 6 | AEP Marketing                                      | Edward P. Cox         | Affirmative |                      |
| 6 | Ameren Energy Marketing Co.                        | Jennifer Richardson   | Affirmative |                      |
| 6 | Bonneville Power Administration                    | Brenda S. Anderson    | Affirmative |                      |
| 6 | Consolidated Edison Co. of New York                | Nickesha P Carrol     | Affirmative |                      |
| 6 | Constellation Energy Commodities Group             | Chris Lyons           | Affirmative |                      |
| 6 | Dominion Resources, Inc.                           | Louis S Slade         | Affirmative |                      |
| 6 | Duke Energy Carolina                               | Walter Yeager         | Affirmative |                      |
| 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  | Negative    | <a href="#">View</a> |
| 6  | Great River Energy   | Donna Stephenson     | Affirmative |                      |
| 6  | Kansas City Power & Light Co.                                | Thomas Saitta        | Negative    | <a href="#">View</a> |
| 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        | Abstain     |                      |
| 6  | New York Power Authority                                     | Thomas Papadopoulos  | Affirmative |                      |
| 6  | Northern Indiana Public Service Co.                          | Joseph O'Brien       | Negative    |                      |
| 6  | PacifiCorp   | Gregory D Maxfield   | Negative    | <a href="#">View</a> |
| 6  | Portland General Electric Co.                                | John Jamieson        |             |                      |
| 6  | Progress Energy  | James Eckelkamp      | Affirmative |                      |
| 6  | PSEG Energy Resources & Trade LLC                            | James D. Hebson      | Affirmative |                      |
| 6  | Public Utility District No. 1 of Chelan County               | Hugh A. Owen         | Affirmative |                      |
| 6  | RRI Energy   | Trent Carlson        | Negative    | <a href="#">View</a> |
| 6  | Salt River Project   | Mike Hummel          |             |                      |
| 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       | Affirmative |                      |
| 6  | Tampa Electric Co.   | Joann Wehle          |             |                      |
| 6  | Western Area Power Administration - UGP Marketing            | John Stonebarger     | Affirmative |                      |
| 6  | Xcel Energy, Inc.  | David F. Lemmons     | Affirmative |                      |
| 8  | Edward C Stein   | Edward C Stein       | Negative    |                      |
| 8  | James A Maenner  | James A Maenner      | Affirmative |                      |
| 8  | JDRJC Associates   | Jim D. Cyrulewski    | Affirmative |                      |
| 8  | Network & Security Technologies                              | Nicholas Lauriat     | Negative    |                      |
| 8  | Power Energy Group LLC                                       | Peggy Abbadini       |             |                      |
| 8  | Roger C Zaklukiewicz   | Roger C Zaklukiewicz | Affirmative |                      |
| 8  | Volkman Consulting, Inc.                                     | Terry Volkman        | Negative    |                      |
| 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     |                      |
| 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         | Affirmative |                      |
| 10 | Electric Reliability Council of Texas, Inc.                  | Kent Saathoff        | Affirmative |                      |
| 10 | Midwest Reliability Organization                             | Dan R Schoenecker    | Affirmative |                      |
| 10 | Northeast Power Coordinating Council, Inc.                   | Guy V. Zito          | Affirmative |                      |
| 10 | ReliabilityFirst Corporation                                 | Jacque Smith         | Affirmative |                      |
| 10 | SERC Reliability Corporation                                 | Carter B Edge        | Affirmative |                      |
| 10 | Western Electricity Coordinating Council                     | Louise McCarren      | Negative    | <a href="#">View</a> |

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-006-01 by PacifiCorp Drafting Team**

**Project 2009-13**

|                   |   |   |
|-------------------|---|---|
|                   | 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   |
| <b>NERC Staff</b> | Scott Mix — Manager Infrastructure Security   | North American Electric Reliability Corporation |
| <b>NERC Staff</b> | Harry Tom — Standards Development Coordinator | North American Electric Reliability Corporation |