January 21, 2010

VIA ELECTRONIC FILING

Lorraine Légère, Board Secretary
New Brunswick Board of Commissioners of Public Utilities
P.O. Box 5001
15 Market Square, Suite 1400
Saint John, NB
E2L 4Y9

Re: *North American Electric Reliability Corporation*

Dear Ms. Légère:

The North American Electric Reliability Corporation ("NERC") hereby submits this Notice of Filing of two interpretations of Critical Infrastructure Protection ("CIP") Reliability Standard CIP-006-2.[1] The interpretations, included as **Exhibits A1 and A2** to this notice, respectively, address Requirements R1.1, and R4 of NERC Reliability Standard CIP-006-2 — Physical Security of Critical Cyber Assets. Both interpretations are appended to the respective standard that is designated as CIP-006-2b in **Exhibit B** to this petition.

The interpretation of Requirement R1.1 was approved by the NERC Board of Trustees on February 12, 2008, and the interpretation of Requirement R4 was approved on August 5, 2009. NERC's notice consists of the following:

[1] At the time these interpretations were submitted to NERC, Version 1 of the CIP standards was the version in effect. The requests were therefore processed referencing CIP-006-1. Since then, CIP-006-2 has been submitted. The changes in CIP-006-2 relative to Version 1 of CIP-006 are not material to the substance of the interpretation request under consideration. In this regard, NERC will append the interpretations to Version 2 of the CIP-006 standard in lieu of Version 1.

- 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-006-2 — Physical Security of Critical Cyber Assets. Requirement R1.1 (**Exhibit A1**);
- Interpretation of CIP-006-2 — Physical Security of Critical Cyber Assets Requirement R4 (**Exhibit A2**);
- Reliability Standard CIP-006-2b — Physical Security of Critical Cyber Assets that includes the appended interpretations of Requirements R1.1 and R4 (**Exhibit B**);
- The complete development records of the Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets, Requirement R1.1 (**Exhibit C1**);
- The complete development records of the Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets, Requirement R4 (**Exhibit C2**); and
- The interpretation development team rosters (**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
MINISTRY OF ENERGY
OF THE PROVINCE OF NEW BRUNSWICK

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF INTERPRETATIONS TO RELIABILITY STANDARD CIP-006-2 — PHYSICAL SECURITY OF CRITICAL CYBER ASSETS, REQUIREMENTS R1.1 AND R4

Gerry 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

January 21, 2010

TABLE OF CONTENTS

I. Introduction 1

II. Notices and Communications 1

III. Background: 2

a. Reliability Standards Development Procedure and Interpretations 2

IV. CIP-006-2 — Physical Security of Critical Cyber Assets Requirement R1.1 4

a. Justification of Interpretation 5

b. Summary of the Reliability Standard Development Proceedings 8

V. CIP-006-2 — Physical Security of Critical Cyber Assets Requirement R4 10

a. Justification of Interpretation 10

b. Summary of the Reliability Standard Development Proceedings 12

Exhibit A1 — Interpretation of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1

Exhibit A2 — Interpretation of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R4

Exhibit B — Reliability Standard CIP-006-2b — Physical Security of Critical Cyber Assets that includes the Appended Interpretations to Requirements R1 and R4

Exhibit C1 — Complete Record of Development of the Interpretation of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1

Exhibit C2 – Complete Record of Development of the Interpretations of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R4

Exhibit D – Interpretation Development Team Rosters

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby submits notice of interpretations of two requirements of NERC Reliability Standard: CIP-006-2 — Physical Security of Critical Cyber Assets, Requirement R1.1 and Requirement R4.

No modification to the language contained in these specific requirements is being proposed through the interpretations. The NERC Board of Trustees approved the interpretation to CIP-006-1[2] — Physical Security of Critical Cyber Assets, Requirement R1.1 on February 12, 2008, and the interpretation of Requirement R4 on August 5, 2009. **Exhibits A1 and A2** to this filing sets forth the interpretations. **Exhibit B** contains the affected Reliability Standard that includes the appended interpretations. **Exhibits C1 and C2** contain the complete development records of the interpretations to CIP-006-1, Requirement.R1.1 and Requirement R4. **Exhibit D** contains the interpretation development team rosters. NERC filed these interpretations with the Federal Energy Regulatory Commission ("FERC") on December 22, 2009, and is filing these interpretations 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:

[2] The NERC Board approved version 2 of CIP-006 on May 6, 2009, which was subsequently approved by FERC on September 30, 2009. Accordingly, the appended interpretations are applied in this filing to version 2 of the CIP-006 standard.

Gerry 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

III. BACKGROUND

a. Reliability Standards Development Procedure and Interpretations

All persons who are directly or materially affected by the reliability of the North American bulk power system are permitted to request an interpretation of a Reliability Standard, as discussed in NERC's *Reliability Standards Development Procedure,* which is incorporated into the Rules of Procedure as Appendix 3A.[3] Upon request, NERC assembles a team with the relevant expertise to address the interpretation request and, within 45 days, presents the interpretation 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 with the applicable governmental authorities. When the affected Reliability Standard is next revised using the *Reliability Standards Development Procedure*, the interpretation will then be incorporated into the Reliability Standard.

The interpretations set out in **Exhibits A1 and A2** have been developed and approved by industry stakeholders using NERC's *Reliability Standards Development*

[3] *See* NERC's *Reliability Standards Development Procedure*, Approved by the NERC Board of Trustees on March 12, 2007, and Effective June 7, 2007 ("Reliability Standards Development Procedure"), available at http://www.nerc.com/files/Appendix3A_StandardsDevelopmentProcess.pdf.

Procedure. The interpretation to Requirement R1.1 was approved by the NERC Board of Trustees on February 12, 2008, and the interpretation to Requirement R4 was approved by the NERC Board of Trustees on August 5, 2009.

During its November 5, 2009 meeting, the NERC Board of Trustees offered guidance regarding interpretations and the interpretations process. As part of this guidance, the NERC Board of Trustees resolved the following:

a. In deciding whether or not to approve a proposed interpretation, the board will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard;

b. It is the expectation of the board that when work on an interpretation reveals a gap or deficiency in a Reliability Standard, stakeholders will take prompt action to address the gap or deficiency in the standard and that the time and effort expended on the interpretation should be a relatively small proportion of the time and effort expended on addressing the gap or deficiency;

c. Priority should be given to addressing deficiencies or gaps in standards that pose a significant risk to the reliability of the bulk power system — addressing the gaps and deficiencies identified in Reliability Standard PRC-005-1 should be given such priority, and the Standards Committee should report on its plans and progress in that regard at the board's February 2010 meeting;

d. The Standards Committee should ensure that the comments by NERC staff and other stakeholders on the proposed interpretations are considered by the standard drafting team in addressing any identified gaps and deficiencies, with a report back to the board on the disposition of those comments;

e. The number of registrants that might end up in non-compliance or the difficulty of compliance are not appropriate inputs to an interpretation process, although those inputs may well be appropriate considerations in a standard development process and development of an implementation plan; and

f. Requests for a decision on how a reliability standard applies to a registered entity's particular facts and circumstances should not be addressed through the interpretations process.

Although the interpretations included in this filing were approved prior to the NERC Board resolution of November 5, 2009, the expectations outlined in the resolution are germane to the interpretations that are the subject of this filing. The NERC Board of Trustees recommended that any gaps or deficiencies in a Reliability Standard that are evident through the interpretation process be addressed promptly by the standard drafting team. NERC has been so advised, and will further examine any gaps or deficiencies in Reliability Standard CIP-006-2 in its consideration of version 4 of this standard through the *Reliability Standards Development Procedure*. This standard is included in the scope of Project 2008-06 — Cyber Security – Order 706 that is currently in process.

IV. CIP-006-2 — Physical Security of Critical Cyber Assets, Requirement R1.1

In Section IV(a) of this filing, NERC explains the need for and development of the formal interpretation to CIP-006-2 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1. NERC believes that the formal interpretation is consistent with the stated reliability goal of the Reliability Standards and the requirements thereunder. Set forth immediately below in Section IV(b) are the stakeholder ballot results and an explanation of how stakeholder comments were considered and addressed by the standard drafting team assembled to provide the interpretation. In this filing, NERC is submitting a proposed interpretation to Requirement R1.1, included as **Exhibit A1**. The Reliability Standard CIP-006-2b — Physical Security of Critical Cyber Assets that includes the Appended Interpretations is included as **Exhibit B**.

The complete development record for the interpretation to R1.1 is set forth in **Exhibit C1**. **Exhibit C1** 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 the interpretation team roster.

a. Justification of Interpretation

CIP-006-2 — Cyber Security — Physical Security of Critical Cyber Assets is "intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2." Requirement R1 of this standard requires the Responsible Entity to document, implement and maintain a physical security plan. Sub-requirement R1.1 specifies that all Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. The specific language of these requirements is:

> **R1.** Physical Security Plan — The Responsible Entity shall document, implement and maintain a physical security plan, approved by a 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 the Critical Cyber Assets.

On August 9, 2007, South Carolina Electric & Gas ("SCE&G") requested that NERC provide a formal interpretation of CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1 and related "Additional Compliance Information" found in Section D.1.4.4 of CIP-006-1.[4] Section D.1.4.4 states, "For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible

[4] Note that in Version 2 of CIP-006, this language is included in Section D.1.5.2.

Entity shall not be required to comply with standard CIP-006 for that single access point at the dial-up device."

In the request for formal interpretation, SCE&G specifically asked:

> *"Are dial-up [remote terminal units (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?"*

NERC assigned the interpretation request to a sub-group of the original CIP standard drafting team that provided the following response:

> *"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 R1.1 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.*
>
> *CIP-006-1 — Additional Compliance Information D.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."*

NERC believes this is a reasonable response to SCE&G's interpretation for two reasons. Importantly, in the first instance, CIP-006-1 was originally developed in the time frame prior to NERC's application to become the ERO. As such, NERC did not have benefit of the current FERC guidance regarding FERC's criteria for approval of Reliability Standards. Then, as now, NERC believes the total intent of the standard is embodied not only in the requirements section itself but in the accompanying sections of the standard that include the title, number, purpose statement, applicability, effective date, measures and various compliance sections. This approach is consistent with the

NERC *Reliability Standards Development Procedure*, currently included in Attachment 3A to the ERO Rules of Procedure, which requires a standard drafting team to develop each of these elements and obtain industry consensus on the standard as a whole.

Accordingly, the NERC standard drafting team that developed CIP-006-1 clearly intended and the industry supported, through demonstration of ballot consensus, Requirement R1 and its sub-part Requirement R1.1, with the *proviso* contained in Section D.1.4.4 that dial-up devices that do not use routable protocols are excepted from the need for a six-wall physical security perimeter. The sub-group drafting team responding to the SCE&G interpretation request validated this as set forth in its response. It is clear from these activities, both the original standard and this interpretation response that independently achieved the required two-thirds weighted segment vote to demonstrate consensus, that the stated response correctly interprets the intent of Requirement R1.1. On this basis, NERC supports the interpretation response that is the subject of this filing.

However, informed at this point by substantial FERC guidance provided since NERC was certified to be the ERO and since the CIP-006-1 standard was originally drafted, NERC fully recognizes the need to revise the language of Requirement R1.1 itself to explicitly identify the exception noted in Section D.1.4.4. NERC commits to doing so as it considers the revision of the CIP family standards in response to FERC's Order No. 706.

NERC believes that the interpretation as presented supports the reliability purpose of the standard, that is, to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Further, the interpretation response recognizes the original intent of the drafting team that developed CIP-006-1 by memorializing the

additional compliance information in Section D.1.4.4. Importantly, this interpretation provides clarity and certainty to SCE&G as it implements its program in support of this important reliability objective. NERC, through its Cyber Security FERC Order No. 706 drafting team, will further consider the issue and impacts identified in this request to determine if improvements are necessary to the requirements to enhance protection of the Bulk Power System. This team is currently developing Version 4 of the Critical Infrastructure Protection standards.

For further perspective, NERC engaged members of the existing Cyber Security FERC Order No. 706 drafting team in July 2009 for an opinion on the issue. The members responded that the referenced additional compliance information (Section D.1.4.4) is supported by language in the CIP-002-1 and CIP-005-1[5] standards and the Version 1 Frequently Asked Questions list that accompany Version 1 of the CIP standards. This information clearly documents the intent of the original standards drafting team: that the Critical Cyber Asset that does not utilize a routable protocol and is "dial-up" accessible shall have a defined Electronic Security Perimeter for that single access point, per CIP-005-1, Requirement R1.2, but is not included in protection requirement of CIP-006-1, Requirement R1.1.

b. Summary of the Reliability Standard Development Proceedings

On August 9, 2007, NERC received a request from SCE&G for an interpretation to Requirement R1.1 of CIP-006-1 — Physical Security of Critical Cyber Assets. NERC assigned the interpretation request to a sub-group of the CIP standard drafting team. NERC conducted an initial ballot of the proposed interpretation from October 18, 2007

[5] The changes included in Version 2 do not substantively change the intent or content of the requirements that are the subject of this interpretation discussion.

through October 29, 2007, and achieved a quorum of 97.37 percent. The ballot also included eleven negative ballots with five associated comments, triggering the need to conduct a recirculation ballot.

- Three balloters indicated agreement with the interpretation, but voted negatively because they felt the interpretation was not needed as the compliance elements of the standard address the question asked in the interpretation.
- One balloter indicated that the CIP Frequently Asked Questions document provided a better response to the request for an interpretation and indicated concern that the interpretation could diminish the purpose of the standard.
- One balloter indicated that the interpretation could create a situation where a Critical Cyber Asset could be left unprotected outside of a Physical Security Perimeter or Electronic Security Perimeter. The sub-group disagreed with this perspective and explained that the interpretation does not eliminate the requirement for an electronic security perimeter.

The sub-group did not modify its interpretation as a result of these comments.

The recirculation ballot was conducted from November 16, 2007 through December 4, 2007 and achieved a final weighted segment approval of 92.62 percent. Nearly 98.7 percent of the registered ballot pool participants voted. Between the initial ballot and the recirculation ballot, several voters changed their ballots, but only one of the changed ballots was accompanied by a comment to explain the reason for the change. There was no discernible pattern in the modifications made, which included:

- Two balloters changed from negative to affirmative;
- Two balloters changed from abstain to affirmative;
- One balloter changed from affirmative to negative;
- One balloter changed from affirmative to abstain;
- One balloter who did not cast an initial ballot cast an affirmative ballot; and
- One balloter who did not cast an initial ballot cast a negative ballot during the recirculation with a comment indicating that although he agreed with

the interpretation, he felt the interpretation was not needed as the response was already provided in the compliance section of the standard.

V. CIP-006-2 — PHYSICAL SECURITY OF CRITICAL CYBER ASSETS, REQUIREMENT R4

In this filing, NERC is submitting a proposed interpretation to Requirement R4 that is included in **Exhibit A2** to this filing. In Section V(a) below, NERC discusses the interpretation, explains the need for, and discusses the development of the formal interpretation to Requirement R4 of CIP-006-2 — Logging Physical Access. NERC also demonstrates that the formal interpretation is consistent with the stated reliability goal of the Reliability Standards and the requirements thereunder. Set forth immediately below in Section V(b) are the stakeholder ballot results and an explanation of how stakeholder comments were considered and addressed by the standard drafting team assembled to provide the interpretation.

The complete development record for the formal interpretation is set forth in **Exhibit C2**, which 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.

a. Justification of Formal Interpretation

The stated purpose of CIP-006-2 — Cyber Security – Physical Security of Critical Cyber Assets is as follows:

> Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

Requirement R4 of this Reliability Standard addresses the need to record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The specific language of Requirement R4 in CIP-006-2 is:

> **R4.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical 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.

On September 12, 2008, the U.S. Army Corps of Engineers ("Corps") requested that NERC provide a formal interpretation of CIP-006-1— Cyber Security – Physical Security of Critical Cyber Assets. Specifically, the Corps requested a formal interpretation for the following inquiries:

- *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
- *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?*

The Corps noted that, "a correct interpretation is needed for entities to determine whether existing systems are fully compliant with this requirement to avoid penalties associated with noncompliance."

NERC assigned its Project 2008-14 Cyber Security Violation Severity Levels Standard Drafting Team ("CSVSL SDT") to respond to the requested interpretation. With respect to the first inquiry, the CSVSL SDT determined that monitoring and logging of access are only required for ingress at this time. With respect to the second question, the CSVSL SDT determined that the term "time of access" refers to the time an authorized individual enters the physical security perimeter.

NERC believes that the interpretation as presented directly supports the reliability purpose of the standard, because it provides clarity and certainty to the requirement that time of access be recorded. NERC also notes that CIP-006 in general and the issues identified in these interpretations specifically are included in the scope of the Cyber Security FERC Order No. 706 drafting team currently developing Version 4 of the Critical Infrastructure Protection standards.

b. Summary of the Reliability Standard Development Proceedings

On September 12, 2008, the Corps requested a formal interpretation of Requirement R4 of CIP-006-1. In accordance with its *Reliability Standard Development Procedure*, NERC posted its response to the request for interpretation for a 30-day pre-ballot period that took place from November 25, 2008 through December 30, 2008. NERC conducted an initial ballot from January 5, 2009 through January 14, 2009. There was a 91.15% quorum with a 97.39% weighted segment vote. Five negative votes were received with three associated comments. This triggered the need to conduct a recirculation ballot after the interpretation team responded to the comments. Accordingly, a recirculation ballot was conducted from February 6, 2009 through

February 16, 2009. The formal interpretation was approved by the ballot pool with a weighted segment average of 99.12%, with 93.81% of the ballot pool voting.

In the comments received, some stakeholders expressed the belief that logging and monitoring should record both ingress time and egress time. Others stated the CIP-002 through CIP-009 Version 1 Standards do not adequately address this area and recommended the matter be turned over to the Project Cyber Security FERC Order 706 Standards Drafting Team for resolution in the next revisions to the CIP Reliability Standards. The standard drafting team responded that the interpretation can only address the requirement as written and that changes to the requirement must be addressed through the standards development process. The standard drafting team also noted that any comments received outside the scope of the interpretation request would be forwarded to the standards drafting team working on revisions to the CIP Reliability Standards. Other commenters suggested that including the phrase "at this time" in the response may imply that the requirement is not adequate as written and may need to be changed in the future. The standard drafting team responded that use of this phrase reflects the fact that the interpretation can only address the requirement as written.

Respectfully submitted,

/s/ Holly A. Hawkins

Gerry 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

Exhibit A1

Interpretation of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1

South Carolina Electric & Gas
Request for Interpretation
August 9, 2007

We would like to request a formal interpretation of CIP-006-1.

CIP-006-1, R1.1. says a physical security plan should address "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."

Also in CIP-006-1, under Additional Compliance Information, 1.4.4 states "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."

The Additional Compliance Information seems to provide an exception to the requirement.

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.

Sally Ballentine Wofford
ERO Compliance Manager

Exhibit A2

Interpretation of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R4

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Request for an Interpretation of a Reliability Standard

Date submitted: **September 12, 2008**

Contact information for person requesting the interpretation:

Name: Karl Bryan

Organization: US Army Corps of Engineers

Telephone: 503-808-3894

E-mail: karl.a.bryan@usace.army.mil

Identify the standard that needs clarification:

Standard Number: CIP-006-1a

Standard Title: Cyber Security — Physical Security of Critical Cyber Assets

Identify specifically what needs clarification

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.

Clarification needed: For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?

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?

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

A correct interpretation is needed for entities to determine whether existing systems are fully compliant with this requirement to avoid penalties associated with noncompliance.

Exhibit B

Reliability Standard CIP-006-2b — Physical Security of Critical Cyber Assets that includes the Appended Interpretations to Requirements R1 and R4

A. Introduction

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

2. Number: CIP-006-2b

3. Purpose: Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-006-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective 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-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

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-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

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-008-2. 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-008-2.

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-006-2 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.

F. Associated Documents

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

2. Appendix 2 – Interpretation of Requirement R4

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Approved by Board of Trustees	New
1a	February 12, 2008	Added Appendix 1: Interpretation of R1 and Additional Compliance Information Section 1.4.4 as approved by the Board of Trustees	Addition
2		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. Replaced the RRO with RE as a responsible entity. 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. 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. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. 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. Changed the Compliance Monitor to Compliance Enforcement Authority.	
2	May 6, 2009	Approved by NERC Board of Trustees	Revised
2b	August 5, 2009	Added Appendix 2: Interpretation of R4 as approved by the Board of Trustees	Addition

Appendix 1

Interpretation of Requirement R1.1. [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.**

[1] The content of the interpretation referenced items that were not substantively changed from Version 1 to Version 2 of the CIP-006 standard and therefore the interpretation is still valid. However, as a result of the transition to Version 2 the requirement numbering was changed such that the references containing the interpretation do not relate to the Version 2 standard. In particular, CIP-006-1 Section 1.4.4 is now labeled Section 1.5.2 in CIP-006-2

Appendix 2

Interpretation of Requirement R4[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.**

[2] The content of the interpretation referenced items that were not substantively changed from Version 1 to Version 2 of the CIP-006 standard and therefore the interpretation is still valid. However, as a result of the transition to Version 2 the requirement numbering was changed such that the references containing the interpretation do not relate to the Version 2 standard. In particular, CIP-006-1 Requirement R4 and its sub parts are now labeled as Requirement R6 in CIP-006-2.

Exhibit C1

Complete Record of Development of the Interpretation of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation — CIP-006 — Physical Security of Critical Cyber Assets (Project 2007-27)

Status:
Approved by the Board of Trustees on February 12, 2008.

Purpose/Industry Need:
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
Interpretation (10) CIP-006-1 Requirement 1.1 and Additional Compliance Information Section 1.4.4	Posted for Board of Trustees Approval	February 12, 2008		
CIP-006-1 Requirement 1.1 and Additional Compliance Information Section 1.4.4 Interpretation (1) Request for Interpretation (2)	Recirculation Ballot Info>> (8) | Vote>>	11/16/07 - 12/04/07 (closed)		Ballot Summary (9)
	Initial Ballot Info>> (4) | Vote>>	10/18/07 - 10/29/07 (closed)	Summary>> (5) Full Record>> (6)	Consideration of Comments>> (7)
	Pre-ballot Review Info>> (3)| Join>>	09/19/07 - 10/18/07 (closed)		

Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets

Request for Interpretation received from South Carolina Electric & Gas on August 9, 2007:
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 provided by a subgroup of CIP Standard Drafting Team members on September 7, 2007:
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.**

South Carolina Electric & Gas
Request for Interpretation
August 9, 2007

We would like to request a formal interpretation of CIP-006-1.

CIP-006-1, R1.1. says a physical security plan should address "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."

Also in CIP-006-1, under Additional Compliance Information, 1.4.4 states "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."

The Additional Compliance Information seems to provide an exception to the requirement.

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.

Sally Ballentine Wofford
ERO Compliance Manager

Maureen E. Long
Standards Process Manager

September 19, 2007

TO: REGISTERED BALLOT BODY

Ladies and Gentlemen:

Announcement: Pre-ballot Windows and Ballot Pools Open September 19, 2007

The Standards Committee (SC) announces the following standards action:

Pre-ballot Window and Ballot Pool for Interpretation of CIP-006-1 (for SCE&G) Opens September 19, 2007

South Carolina Electric & Gas Company submitted a Request for an Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets. The request asked if dial-up remote terminal units (RTUs) that use non-routable protocols and have dial-up access are required to have six-wall perimeters or are only required to have electronic security perimeters.

The Interpretation clarifies that if dial-up assets are classified as critical cyber assets in accordance with CIP-002-1, the assets 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. Entities are not required to enclose dial-up RTUs that do not use routable protocols within a six-wall border.

A new ballot pool to vote on this interpretation has been formed and will remain open up until 8 a.m. (EDT) on Thursday, October 18, 2007. During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." The list server for this ballot pool is: bp-interp_cip-006_sceg_in@nerc.com

The initial ballot for this interpretation will begin at 8 a.m. (EDT) on Thursday, October 18, 2007.

Pre-ballot Window and Ballot Pool for Interpretation of BAL-005 Requirement R17 (for PGE) Opens September 19, 2007

Portland General Electric Company submitted a Request for an Interpretation of BAL-005-1 — Automatic Generation Control Requirement R17. The request asked if the requirement to annually check and calibrate time error and frequency devices applies to the following measuring devices:

- Only equipment within the operations control room
- Only equipment that provides values used to calculate automatic generation control area control error
- Only equipment that provides values to its SCADA system
- Only equipment owned or operated by the balancing authority
- Only to new or replacement equipment

- To all equipment that a balancing authority owns or operates

The Interpretation clarifies that Requirement R17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the ACE equation or provide real-time time error or frequency information to the system operator. The time error and frequency measurement devices may not necessarily be located in the operations control room or owned by the balancing authority; however, the balancing authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in Requirement 17.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

A new ballot pool to vote on this interpretation has been formed and will remain open up until 8 a.m. (EDT) on Thursday, October 18, 2007. During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." The list server for this ballot pool is: bp-interp_bal-005_pge_in@nerc.com

The initial ballot for this interpretation will begin at 8 a.m. (EDT) on Thursday, October 18, 2007.

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. If you have any questions, please contact me at 813-468-5998 or maureen.long@nerc.net.

Sincerely,

Maureen E. Long

cc: Registered Ballot Body Registered Users
Standards Mailing List
NERC Roster

Maureen E. Long
Standards Process Manager

October 18, 2007

TO: REGISTERED BALLOT BODY

Ladies and Gentlemen:

Announcement: Initial Ballot Windows, Pre-ballot Review Period, and Ballot Pool Open

The Standards Committee (SC) announces the following standards actions:

Initial Ballot Window for Urgent Action Revisions to BAL-004 is Open

The NERC Operating Committee has submitted an Urgent Action SAR to revise BAL-004-0 — Time Error Correction to remove the following from BAL-004:

- **Requirement 1, second sentence:** A single Reliability Coordinator in each Interconnection shall be designated by the NERC Operating Committee to serve as Interconnection Time Monitor.
  - **Reason for removal:** The entities who have been serving as the Interconnection Time Monitors have done so voluntarily. The NERC Operating Committee is not a user, owner, or operator and has no authority to assign a reliability coordinator to serve as the Interconnection Time Monitor. The entities who have been serving as "volunteers" don't want to continue to serve in this role if they are subject to sanctions for non-compliance with Requirement 2, which supports a business practice.
- **Requirement 2:** The Interconnection Time Monitor shall monitor Time Error and shall initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
  - **Reason for removal:** This requires the reliability coordinator to execute a time error correction in accordance with a NAESB business practice.

The initial ballot for the Urgent Action revisions to BAL-004 is open and will remain open until 8 p.m. on Monday, October 29, 2007.

Initial Ballot Window for Interpretation of CIP-006-1 (for SCE&G) is Open

South Carolina Electric & Gas Company submitted a Request for an Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets. The request asked if dial-up remote terminal units (RTUs) that use non-routable protocols and have dial-up access are required to have six-wall perimeters or are only required to have electronic security perimeters.

The Interpretation clarifies that if dial-up assets are classified as critical cyber assets in accordance with CIP-002-1, the assets 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. Entities are not required to enclose dial-up RTUs that do not use routable protocols within a six-wall border.

The initial ballot for the interpretation of CIP-006-1 is open and will remain open until 8 p.m. on Monday, October 29, 2007.

Initial Ballot Window for Interpretation of BAL-005 Requirement R17 (for PGE) is Open

Portland General Electric Company submitted a Request for an Interpretation of BAL-005-1 Automatic Generation Control Requirement R17. The Interpretation asked if the requirement to annually check and calibrate time error and frequency devices applies to the following measuring devices:

- Only equipment within the operations control room
- Only equipment that provides values used to calculate automatic generation control area control error
- Only equipment that provides values to its SCADA system
- Only equipment owned or operated by the balancing authority
- Only to new or replacement equipment
- To all equipment that a balancing authority owns or operates

The Interpretation clarifies that Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the ACE equation or provide real-time time error or frequency information to the system operator. The time error and frequency measurement devices may not necessarily be located in the operations control room or owned by the balancing authority; however, the balancing authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in Requirement 17.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

The initial ballot for this interpretation of BAL-005 Requirement 17 is open and will remain open until 8 p.m. on Monday, October 29, 2007.

Pre-ballot Window and Ballot Pool for PRC-023-1 — Relay Loadability Opens October 18, 2007

A new standard, PRC-023-1 — Relay Loadability, is posted for a 30-day pre-ballot review through 8 a.m. on November 19, 2007.

This standard was developed to address the cascading transmission outages that occurred in the August 2003 blackout when backup distance and phase relays operated on high loading and low voltage without electrical faults on the protected lines. This is the so-called ‘zone 3 relay’ issue that has been expanded to address other protection devices subject to unintended operation during extreme system conditions. The proposed standard establishes minimum loadability criteria for these relays to minimize the chance of unnecessary line trips during a major system disturbance.

The ballot for this standard will also include the Relay Loadability Implementation Plan.

The ballot pool to vote on this standard was formed earlier this year and has been re-opened. Anyone who joined the ballot pool earlier this year and is still a valid member of the Registered Ballot Body will not need to re-join the ballot pool. The ballot pool will remain open until 8 a.m. Monday, November 19, 2007. During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." The list server for this ballot pool is:

bp-Relay Loadability_in@nerc.com

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. If you have any questions, please contact me at 813-468-5998 or maureen.long@nerc.net.

Sincerely,

Maureen E. Long

cc: Registered Ballot Body Registered Users
Standards Mailing List
NERC Roster

Maureen E. Long
Standards Process Manager

October 31, 2007

TO: REGISTERED BALLOT BODY

Ladies and Gentlemen:

Announcement of Initial Ballot Results for Three Ballots

The Standards Committee (SC) announces the following:

Initial Ballot Results for Urgent Action Revisions to BAL-004-0

The initial ballot for the Urgent Action Revisions to BAL-004-0 — Time Error Correction was conducted from October 18 through October 29, 2007. The proposed revision removes the following from BAL-004:

- **Requirement 1, second sentence:** A single Reliability Coordinator in each Interconnection shall be designated by the NERC Operating Committee to serve as Interconnection Time Monitor.
  - **Reason for removal:** The entities who have been serving as the Interconnection Time Monitors have done so voluntarily. The NERC Operating is not a user, owner, or operator and has n authority to assign a reliability coordinator to serve as the Interconnection Time Monitor. The entities who have been serving as 'volunteers' don't want to continue to serve in this role if they are subject to sanctions for non-compliance with Requirement 2, which supports a business practice.
- **Requirement 2:** The Interconnection Time Monitor shall monitor Time Error and shall initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
  - **Reason for removal:** This requires the reliability coordinator to execute a time error correction in accordance with a NAESB business practice.

The ballot achieved a quorum; however, there were some negative ballots with comments, initiating the need to undergo a re-circulation ballot. The drafting team will be reviewing comments submitted with the ballot and preparing its consideration of those comments. (Detailed Ballot Results)

Quorum: 96.18 %
Approval: 93.93 %

Initial Ballot Results for Interpretation of CIP-006-1 (for SCE&G)

The initial ballot for the Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets was conducted from October 18 through October 29, 2007. The request for an interpretation asked if dial-up remote terminal units (RTUs) that use non-routable protocols and have dial-up access are required to have six-wall perimeters or are only required to have electronic security perimeters.

The Interpretation clarifies that if dial-up assets are classified as critical cyber assets in accordance with CIP-002-1, the assets 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. Entities are not required to enclose dial-up RTUs that do not use routable protocols within a six-wall border.

The ballot achieved a quorum; however, there were some negative ballots with comments, initiating the need to undergo a re-circulation ballot. The drafting team will be reviewing comments submitted with the ballot and preparing its consideration of those comments. (Detailed Ballot Results)

Quorum: 97.37%
Approval: 92.24%

Initial Ballot Results for Interpretation of BAL-005 Requirement R17 (for PGE)

The initial ballot for the Interpretation of BAL-005-1 — Automatic Generation Control Requirement R17 was conducted from October 18 through October 29, 2007. The request for an interpretation asked if the requirement to annually check and calibrate time error and frequency devices applies to the following measuring devices:

- Only equipment within the operations control room
- Only equipment that provides values used to calculate automatic generation control area control error
- Only equipment that provides values to its SCADA system
- Only equipment owned or operated by the balancing authority
- Only to new or replacement equipment
- To all equipment that a balancing authority owns or operates

The Interpretation clarifies that Requirement R17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the ACE equation or provide real-time time error or frequency information to the system operator. The time error and frequency measurement devices may not necessarily be located in the operations control room or owned by the balancing authority; however, the balancing authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in Requirement 17.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

The ballot achieved a quorum however there were some negative ballots with comments, initiating the need to undergo a re-circulation ballot. The drafting team will be reviewing comments submitted with the ballot and preparing its consideration of those comments. (Detailed Ballot Results)

Quorum: 96.48%
Approval: 85.91%

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. If you have any questions, please contact me at 813-468-5998 or maureen.long@nerc.net.

Sincerely,

Maureen E. Long

cc: Registered Ballot Body Registered Users
Standards Mailing List
NERC Roster

Reliability Standards

User Name

Password

Log in

Register

Reliability Standards Home
Announcements
BOT Approved Standards
Regulatory Approved Standards
Standards Under Development
Ballot Pools
Current Ballots
Ballot Results
Registered Ballot Body
Proxy Voters
Registration Instructions
Regional Reliability Standards

NERC Home

Ballot Results	
Ballot Name:	Interpretation Request - CIP-006 - SCE&G_in
Ballot Period:	10/18/2007 - 10/29/2007
Ballot Type:	Initial
Total # Votes:	148
Total Ballot Pool:	152
Quorum:	97.37 % The Quorum has been reached
Weighted Segment Vote:	92.24 %
Ballot Results:	The standard will proceed to recirculation ballot.

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	45	1	39	0.929	3	0.071	3	0
2 - Segment 2.	7	0.5	5	0.5	0	0	2	0
3 - Segment 3.	35	1	31	0.912	3	0.088	1	0
4 - Segment 4.	8	0.8	8	0.8	0	0	0	0
5 - Segment 5.	25	1	20	0.909	2	0.091	1	2
6 - Segment 6.	17	1	15	0.938	1	0.063	0	1
7 - Segment 7.	1	0.1	1	0.1	0	0	0	0
8 - Segment 8.	2	0.1	1	0.1	0	0	1	0
9 - Segment 9.	4	0.4	4	0.4	0	0	0	0
10 - Segment 10.	8	0.7	5	0.5	2	0.2	0	1
Totals	152	6.6	129	6.088	11	0.513	8	4

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services Company	Kirit S. Shah	Affirmative	
1	American Public Power Association	E. Nick Henery	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Arizona Public Service Co.	Cary B. Deise	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Doug Hils	Affirmative	
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	

1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Julien Gagnon	Affirmative	
1	JEA	Ted E. Hobson	Affirmative	
1	Kansas City Power & Light Co.	Jim Useldinger	Affirmative	
1	Lincoln Electric System	Doug Bantam	Negative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Robert G. Coish	Affirmative	
1	Minnesota Power, Inc.	Carol Gerou	Negative	
1	National Grid USA	Herbert Schrayshuen	Affirmative	
1	Nebraska Public Power District	Richard L. Koch	Affirmative	
1	New Brunswick Power Transmission Corporation	Wayne N. Snowdon	Affirmative	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Joseph Dobes	Abstain	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	PacifiCorp	Robert Williams	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Sacramento Municipal Utility District	Dilip Mahendra	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Linda Brown	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SaskPower	Wayne Guttormson	Affirmative	
1	Seattle City Light	Christopher M. Turner	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Tri-State G & T Association Inc.	Bruce A Sembrick	Affirmative	
1	Tucson Electric Power Co.	Ronald P. Belval	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
2	Alberta Electric System Operator	Anita Lee	Abstain	View
2	California ISO	David Hawkins	Affirmative	
2	Independent Electricity System Operator	Don Tench	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Abstain	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
3	Alabama Power Company	Robin Hurst	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Tallahassee	Rusty S. Foster	Negative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consumers Energy Co.	David A. Lapinski	Affirmative	View
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	Farmington Electric Utility System	Alan Glazner	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen	Affirmative	

		Borrell		
3	Florida Municipal Power Agency	Michael Alexander	Affirmative	
3	Florida Power Corporation	Lee Schuster	Abstain	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia Transmission Corporation	William Neil Phinney	Affirmative	
3	Great River Energy	Sam Kokkinen	Negative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Lincoln Electric System	Bruce Merrill	Negative	View
3	Manitoba Hydro	Ronald Dacombe	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters	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 Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Tennessee Valley Authority	Cynthia Herron	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	American Municipal Power - Ohio	Chris Norton	Affirmative	
4	Consumers Energy Co.	David Frank Ronk	Affirmative	View
4	Florida Municipal Power Agency	William S. May	Affirmative	
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 2 of Grant County	Kevin J. Conway	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Power	Pamela Pahl	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Conectiv Energy Supply, Inc.	Richard K. Douglass	Affirmative	
5	Constellation Generation Group	Michael F. Gildea	Abstain	
5	Dynegy	Greg A. Mason	Affirmative	
5	Exelon Corporation	Jack Crowley	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	Douglas Keegan	Affirmative	
5	Great River Energy	Cynthia E Sulzer	Negative	
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	Municipal Electric Authority of Georgia	Roger Brand	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	Reliant Energy Services	Thomas J. Bradish	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Southern Company Services, Inc.	Roger D. Green	Affirmative	
5	TXU Generation Company LP	Rickey Terrill		

5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Xcel Energy, Inc.	Stephen J. Beuning	Affirmative	
6	AEP Service Corp.	Dana E. Horton	Affirmative	
6	Black Hills Power	Larry Williamson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Entergy Services, Inc.	William Franklin	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	First Energy Solutions	Alfred G. Roth	Affirmative	
6	Florida Municipal Power Agency	Robert C. Williams		
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Luminant Energy	Thomas Burke	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	PP&L, Inc.	Thomas Hyzinski	Affirmative	
6	Progress Energy Carolinas	James Eckelkamp	Affirmative	
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	South Carolina Electric & Gas Co.	John E Folsom, Jr.	Affirmative	
6	Southern Company Generation and Energy Marketing	J. Roman Carter	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
7	Eastman Chemical Company	Lloyd Webb	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Public Service Commission	James T. Gallagher	Affirmative	
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Negative	View
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Larry Brusseau		
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Edward A. Schwerdt	Affirmative	
10	SERC Reliability Corporation	Gerry W. Cauley	Affirmative	
10	Southwest Power Pool	Charles H. Yeung	Negative	View
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

609.452.8060 (Voice) - 609.452.9550 (Fax)
116-390 Village Boulevard, Princeton, New Jersey 08540-5721

Consideration of Comments on Initial Ballot of Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets for South Carolina Electric and Gas

Summary Consideration: The drafting team did not make any changes to the interpretation based on the comments submitted with the initial ballot of the interpretation of CIP-006-1.

Organization:	**Alberta Electric System Operator**
Member:	Anita Lee
Comment:	This interpretation is rendered awkward due to the highly prescriptive nature of the CIP-006 standard. The standard overlooks the overall objective, that being adequate physical security for critical cyber assets, and attempts to addresses details that mislead the safeguard selection process. Specifically, the matter of routable protocols being used by the critical cyber asset is not particularly salient to the determination of the adequacy of physical security measures. Furthermore, prescribing a six-wall border compounds the difficulty of arriving at an appropriate conclusion, by forcing even more implementation level detail into consideration. Consequently, on one hand, the interpretation seems acceptable, in the sense that a six-wall border is not absolutely necessary for dialup RTUs that do not use routable protocols. However, this point is specious, since the same could be said for any critical cyber asset. If appropriate alternative measures are in place to provide physical security, then the use of routable protocols and the presence of six-wall borders are unnecessary details and should therefore not be considered at the level of a generic, mandatory standard. However, on the other hand, the interpretation is not acceptable, in the sense that it fails to indicate that appropriate physical security measures must be implemented, regardless of the use or lack of routable protocols. This ambivalence is caused directly by the standard approaching a level of detail that can only be properly considered in a specific circumstance, not in the general case.
Response:	While the comments directed at the standard are appreciated, the interpretation focuses on the standard as approved. The interpretation is consistent with the set of cyber security standards in that it provides a balanced solution between not having any protection (as would be the case for a non-dial-up, non-routable connection), and “full” protection for a permanently-connected routable protocol connection.
Organization:	**Consumers Energy Co.**
Member:	David A. Lapinski
Member:	David Frank Ronk
Comment:	We are voting in favor of this interpretation, but we recommend that the phrase, “and they must reside within an Electronic Security Perimeter” should be omitted. This interpretation is nominally related only to CIP-006-1. This phrase seems to bring CIP-005 into the scope of the interpretation. It appears that the phrase was included solely for illustrative reasons in the original interpretation request. Repeating it in the formal interpretation, however, raises a number of concerns regarding CIP-005 interpretation. We believe these are unintended and may be inconsistent with CIP-005 and its associated explanatory documentation (such as the FAQ's).
Response:	The phrase was included for illustrative purposes to remind the reader that Electronic Security is still required. For compliance purposes, only the requirements of CIP-005 may be used to assess compliance. CIP-006, its interpretation, or any element of the

	FAQ cannot be used to establish new requirements, or to assess compliance.
Organization:	**Lincoln Electric System**
Member:	Bruce Merrill
Member:	Dennis Florom
Comment:	LES agrees with the interpretation as written, however it is not needed. As the Interpretation team has correctly pointed out, South Carolina Electric & Gas's query is already addressed in Additional Compliance Information 1.4.4 of the standard. Per the Reliability Standards Development Procedure, a interpretation will stand with the approved standard until the standard is revised thorough the normal process, at which time the standard will be modified to incorporate the clarifications. It seems unnecessary for this Interpretation to stand with the currently approved standard and additionally no modifications to the approved standard appear to be needed as a result of this Interpretation.
Response:	The formal Request for Interpretation process obliges NERC to prepare, post for review and ballot a response to the request. The requestor sought a formal interpretation therefore the process was initiated and followed. The resultant interpretation response confirmed the intent of the drafting team, and may be used during revisions of the CIP-006 standard as justification for clearing up any language or confusion in the standard.
Organization:	**Electric Reliability Council of Texas, Inc.**
Member:	Kent Saathoff
Comment:	The interpretation should not be approved because it could create a situation where a Critical Cyber Asset could be left unprotected outside of a Physical Security Perimeter or Electronic Security Perimeter.
Response:	The interpretation does not eliminate the requirement for an Electronic Security Perimeter (in specifically reminds the reader that the assets must reside within an Electronic Security Perimeter). The interpretation is consistent with the set of cyber security standards in that it provides a compromise solution between not having any protection (as would be the case for a non-dial-up, non-routable connection), and “full” protection for a permanently-connected routable protocol connection.
Organization:	**Southwest Power Pool**
Member:	Charles H. Yeung
Comment:	There is an alternative already identified in CIP-006 that SCE&G can apply to its dial-up RTUs in a facility that is difficult to secure. From Page 18 of the CIP standards FAQ: Standard CIP–006–1 — Cyber Security — Physical Security 1. Question: What is a “six-wall” border? Answer: This refers to a physical, completely enclosed border, such as a room, cage, safe, or metal cabinet. Raised floors and drop ceilings may not constitute part of a border because they could create potentially uncontrolled access points. Fences do not constitute a completely enclosed border. The intent is to clearly define a security boundary that applies the same level of security over its entire area. However, SPP is aware that this interpretation may be based on wording from Sec D. Compliance: 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. SPP is concerned that D.1.4.4 and the interpretation diminishes the purpose of CIP-

	006, whereas the FAQ quoted provides appropriate cyber security protection and a reasonable solution for securing a dial-up RTU that is recognized by the registered entity to be a critical cyber asset. Compliance information should not be applied to contradict the purpose of the standard itself. Although the interpretation is limited to the existing standards language, and the NERC standards process should be used to submit a standards change, SPP does not support this interpretation.
Response:	The requestor sought a formal response to its request for interpretation. The interpretation is based in the language of the Compliance section noted. The FAQ is an informational-only document, and does not contain any requirements. Since the interpretation is based on language already included in the standard, there are no new requirements or changes to existing requirements.

Maureen E. Long
Standards Process Manager

November 16, 2007

TO: REGISTERED BALLOT BODY

Ladies and Gentlemen:

Announcement: Recirculation Ballot Windows Open

The Standards Committee (SC) announces the following standards actions:

Recirculation Ballot Window for Urgent Action Revisions to BAL-004-0 is Open

The recirculation ballot for the Urgent Action revisions to BAL-004-0 — Time Error Correction requested by the NERC Operating Committee is open through 8 p.m. (EST) Tuesday, December 4, 2007. The Standards Committee encourages all members of the Ballot Pool to review the Operating Committee's consideration of initial ballot comments.

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.

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.

Recirculation Ballot Window for Interpretation of CIP-006-1 (for SCE&G) is Open

The recirculation ballot for the Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets requested by South Carolina Electric & Gas Company is open through 8 p.m. (EST) Tuesday, December 4, 2007. The Standards Committee encourages all members of the Ballot Pool to review the drafting team's consideration of initial ballot comments.

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.

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.

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. If you have any questions, please contact me at 813-468-5998 or maureen.long@nerc.net.

Sincerely,

Maureen E. Long

cc: Registered Ballot Body Registered Users
Standards Mailing List
NERC Roster

Reliability Standards

User Name

Password

Log in

Register

Reliability Standards Home
Announcements
BOT Approved Standards
Regulatory Approved Standards
Standards Under Development
Ballot Pools
Current Ballots
Ballot Results
Registered Ballot Body
Proxy Voters
Registration Instructions
Regional Reliability Standards

NERC Home

Ballot Results	
Ballot Name:	Interpretation Request - CIP-006 - SCE&G_rc
Ballot Period:	11/16/2007 - 12/4/2007
Ballot Type:	recirculation
Total # Votes:	151
Total Ballot Pool:	153
Quorum:	98.69 % The Quorum has been reached
Weighted Segment Vote:	92.62 %
Ballot Results:	The Standard has Passed

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	45	1	39	0.907	4	0.093	2	0
2 - Segment 2.	7	0.5	5	0.5	0	0	2	0
3 - Segment 3.	35	1	32	0.941	2	0.059	1	0
4 - Segment 4.	8	0.8	8	0.8	0	0	0	0
5 - Segment 5.	25	1	20	0.909	2	0.091	1	2
6 - Segment 6.	17	1	16	0.941	1	0.059	0	0
7 - Segment 7.	1	0.1	1	0.1	0	0	0	0
8 - Segment 8.	2	0.1	1	0.1	0	0	1	0
9 - Segment 9.	5	0.5	5	0.5	0	0	0	0
10 - Segment 10.	8	0.8	6	0.6	2	0.2	0	0
Totals	153	6.8	133	6.298	11	0.502	7	2

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services Company	Kirit S. Shah	Affirmative	
1	American Public Power Association	E. Nick Henery	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Arizona Public Service Co.	Cary B. Deise	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Doug Hils	Affirmative	
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	

1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Abstain	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Julien Gagnon	Affirmative	
1	JEA	Ted E. Hobson	Affirmative	
1	Kansas City Power & Light Co.	Jim Useldinger	Affirmative	
1	Lincoln Electric System	Doug Bantam	Negative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Robert G. Coish	Affirmative	
1	Minnesota Power, Inc.	Carol Gerou	Negative	
1	National Grid USA	Herbert Schrayshuen	Affirmative	
1	Nebraska Public Power District	Richard L. Koch	Affirmative	
1	New Brunswick Power Transmission Corporation	Wayne N. Snowdon	Affirmative	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Joseph Dobes	Affirmative	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Negative	
1	PacifiCorp	Robert Williams	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Sacramento Municipal Utility District	Dilip Mahendra	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Linda Brown	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SaskPower	Wayne Guttormson	Affirmative	
1	Seattle City Light	Christopher M. Turner	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Tri-State G & T Association Inc.	Bruce A Sembrick	Affirmative	
1	Tucson Electric Power Co.	Ronald P. Belval	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
2	Alberta Electric System Operator	Anita Lee	Abstain	View
2	California ISO	David Hawkins	Affirmative	
2	Independent Electricity System Operator	Don Tench	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Abstain	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
3	Alabama Power Company	Robin Hurst	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Tallahassee	Rusty S. Foster	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consumers Energy Co.	David A. Lapinski	Affirmative	View
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	Farmington Electric Utility System	Alan Glazner	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen	Affirmative	

		Borrell		
3	Florida Municipal Power Agency	Michael Alexander	Affirmative	
3	Florida Power Corporation	Lee Schuster	Abstain	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia Transmission Corporation	William N Phinney	Affirmative	
3	Great River Energy	Sam Kokkinen	Negative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Lincoln Electric System	Bruce Merrill	Negative	View
3	Manitoba Hydro	Ronald Dacombe	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters	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 Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Tennessee Valley Authority	Cynthia Herron	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	American Municipal Power - Ohio	Chris Norton	Affirmative	
4	Consumers Energy Co.	David Frank Ronk	Affirmative	View
4	Florida Municipal Power Agency	William S. May	Affirmative	
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 2 of Grant County	Kevin J. Conway	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Power	Pamela Pahl	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Conectiv Energy Supply, Inc.	Richard K. Douglass	Affirmative	
5	Constellation Generation Group	Michael F. Gildea	Abstain	
5	Dynegy	Greg Mason	Affirmative	
5	Exelon Corporation	Jack Crowley	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	Douglas Keegan	Affirmative	
5	Great River Energy	Cynthia E Sulzer	Negative	
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	Municipal Electric Authority of Georgia	Roger Brand	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	Reliant Energy Services	Thomas J. Bradish	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Southern Company Services, Inc.	Roger D. Green	Affirmative	
5	TXU Generation Company LP	Rickey Terrill		

5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Xcel Energy, Inc.	Stephen J. Beuning	Affirmative	
6	AEP Service Corp.	Dana E. Horton	Affirmative	
6	Black Hills Power	Larry Williamson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Entergy Services, Inc.	William Franklin	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	First Energy Solutions	Alfred G. Roth	Affirmative	
6	Florida Municipal Power Agency	Robert C. Williams	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Luminant Energy	Thomas Burke	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	PP&L, Inc.	Thomas Hyzinski	Affirmative	
6	Progress Energy Carolinas	James Eckelkamp	Affirmative	
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	South Carolina Electric & Gas Co.	John E Folsom, Jr.	Affirmative	
6	Southern Company Generation and Energy Marketing	J. Roman Carter	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
7	Eastman Chemical Company	Lloyd Webb	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Public Service Commission	James T. Gallagher	Affirmative	
9	Wyoming Public Service Commission	Steve Oxley	Affirmative	
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Larry Brusseau	Negative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Edward A. Schwerdt	Affirmative	
10	SERC Reliability Corporation	Gerry W. Cauley	Affirmative	
10	Southwest Power Pool	Charles H. Yeung	Negative	View
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

609.452.8060 (Voice) - 609.452.9550 (Fax)
116-390 Village Boulevard, Princeton, New Jersey 08540-5721

Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets

Request for Interpretation received from South Carolina Electric & Gas on August 9, 2007:
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 provided by a subgroup of CIP Standard Drafting Team members on September 7, 2007:
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.**

Exhibit C2

Complete Record of Development of the Interpretations of Reliability Standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R4

Project 2008-15

Interpretation – CIP-006-1a, R4 – Cyber Security — Physical Security of Critical Cyber Assets

Related Files

Status: An interpretation of CIP-006-01a, Requirement R4 for the US Army Corps of Engineers was posted for a 10-day recirculation ballot. The ballot pool approved the interpretation and it will now be submitted to the NERC Board of Trustees for adoption.

Summary: The request asks to clarify requirements for monitoring and logging physical access referenced in Requirement R4.

Purpose / Industry Need: 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
US Army Corps of Engineers Request for Interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets Interpretation (1) Request for Interpretation (2) CIP-006-1a (3)	Recirculation Ballot Info>> (9) | Vote>>	02/06/09 - 02/16/09 (closed)	Summary>> (10) Full Record>> (11)	
	Initial Ballot Info>> (5) | Vote>>	01/05/09 - 01/14/09 (closed)	Summary>> (6) Full Record>> (7)	Consideration of Comments>> (8)
	Pre-ballot Review Info>> (4) | Join>>	11/25/08-12/30/08 (closed)		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Request for an Interpretation of a Reliability Standard

Date submitted: **September 12, 2008**

Contact information for person requesting the interpretation:

Name: Karl Bryan

Organization: US Army Corps of Engineers

Telephone: 503-808-3894

E-mail: karl.a.bryan@usace.army.mil

Identify the standard that needs clarification:

Standard Number: CIP-006-1a

Standard Title: Cyber Security — Physical Security of Critical Cyber Assets

Identify specifically what needs clarification

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.

Clarification needed: For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?

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?

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or

an incorrect interpretation of this standard.

A correct interpretation is needed for entities to determine whether existing systems are fully compliant with this requirement to avoid penalties associated with noncompliance.

Project 2008-15: Interpretation of CIP-006-1a, Requirement R4 for the US Army Corps of Engineers

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.

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.

Question #1

For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?

Response to Question #1

No, monitoring and logging of access are only required for ingress at this time.

Question #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?

Response to Question #2

The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Request for an Interpretation of a Reliability Standard

Date submitted: **September 12, 2008**

Contact information for person requesting the interpretation:

Name: Karl Bryan

Organization: US Army Corps of Engineers

Telephone: 503-808-3894

E-mail: karl.a.bryan@usace.army.mil

Identify the standard that needs clarification:

Standard Number: CIP-006-1a

Standard Title: Cyber Security — Physical Security of Critical Cyber Assets

Identify specifically what needs clarification

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.

Clarification needed: For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?

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?

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

A correct interpretation is needed for entities to determine whether existing systems are fully compliant with this requirement to avoid penalties associated with noncompliance.

A. Introduction

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

2. Number: CIP-006-1a

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

4. Applicability:

4.1. Within the text of Standard CIP-006, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

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

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

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

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

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

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

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

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

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

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

R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

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

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

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

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

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms

for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

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

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

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

R5. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

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

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

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

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

C. Measures

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

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

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

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

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

Access logs as specified in Requirement R5.

Documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

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

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

1.4. Additional Compliance Information

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

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

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

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

2. Levels of Noncompliance

2.1. Level 1:

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

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

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

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

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

2.1.6 One required document does not exist.

2.2. Level 2:

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

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

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

2.2.4 More than one required document does not exist.

2.3. Level 3:

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

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

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

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

2.4.3 No maintenance or testing program exists.

E. Regional Differences

None identified.

F. Associated Documents

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

Version History

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

Appendix 1

Interpretation of Requirement R1.1.

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

Interpretation:

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

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

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

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

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

1.4. Additional Compliance Information

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool and Pre-ballot Window
November 25–December 30, 2008

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

Interpretation of CIP-006-01a for the US Army Corps of Engineers (Project 2008-15)

An interpretation of CIP-006-01a, Requirement R4 for the US Army Corps of Engineers 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 p.m. EST on December 30, 2008**. Voting will begin on or after January 5, 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-RFI_CIP-006-1a_Army_in.

Background

The US Army Corps of Engineers requested an interpretation to clarify requirements for monitoring and logging physical access referenced in Requirement R4. The request and interpretation can be found the project page: http://www.nerc.com/filez/standards/Project2008-15_Interpretation_CIP-006-1a_US_Army_COE.html

Standards Development Process

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Two Initial Ballot Windows Open

January 5–14, 2009

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

Initial ballot windows for the following projects are now open until 8 p.m. EST on January 14, 2009:

Revisions to Violation Severity Levels for TOP-004-2 — Transmission Operations (Project 2008-16)

The proposed Violation Severity Levels support changes to TOP-004-1 requirements that were approved as part of the FAC-010-1, FAC-011-1, and FAC-014-1 project.

The status, purpose, and supporting documents for this project are posted on the project page: http://www.nerc.com/filez/standards/Project_2008-16_Trans_Ops_VSLs.html

Interpretation of CIP-006-1a Requirement R4 for the US Army Corps of Engineers (Project 2008-15)

The US Army Corps of Engineers requested an interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets to clarify requirements for monitoring and logging physical access referenced in Requirement R4.

The request and interpretation are posted on the project page: http://www.nerc.com/filez/standards/Project2008-15_Interpretation_CIP-006-1a_US_Army_COE.html

Standards Development Process

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Results

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

Initial Ballots:

Revisions to Violation Severity Levels for TOP-004-2 — Transmission Operations (Project 2008-16)

Since at least one negative ballot was submitted with a comment, a recirculation ballot will be held. The recirculation ballot will be held after the drafting team responds to voter comments submitted during this ballot.

The initial ballot for revisions to Violation Severity Levels for TOP-004-2 — Transmission Operations ended January 14, 2008. The ballot results are shown below. The Ballot Results Web page provides a link to the detailed results.

Quorum: 91.20 %
Approval: 93.93 %

Project page: http://www.nerc.com/filez/standards/Project_2008-16_Trans_Ops_VSLs.html

Interpretation of CIP-006-1a Requirement R4 for the US Army Corps of Engineers (Project 2008-15)

Since at least one negative ballot was submitted with a comment, a recirculation ballot will be held. The recirculation ballot will be held after the drafting team responds to voter comments submitted during this ballot.

The initial ballot for an interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets Requirement R4 (requested by the US Army Corps of Engineers) ended January 14, 2008. The ballot results are shown below. The Ballot Results Web page provides a link to the detailed results.

Quorum: 91.15 %
Approval: 97.39 %

Project page: http://www.nerc.com/filez/standards/Project2008-15_Interpretation_CIP-006-1a_US_Army_COE.html

Recirculation Ballots:

Interpretation of VAR-002-1a for ICF Consulting (Project 2008-11)

The ballot has passed and will be submitted to the NERC Board of Trustees for approval.

The recirculation ballot for the interpretation of VAR-002-1a — Generator Operation for Maintaining Network Voltage Schedules (requested by ICF Consulting) ended January 15, 2009. The final ballot results are shown below. The Ballot Results Web page provides a link to the detailed results.

Quorum: 91.47 %
Approval: 91.21 %

Project page: http://www.nerc.com/filez/standards/Project2008-11_VAR-002_Interpretation.html

Interpretation of EOP-001-0 Requirement R1 for Regional Entity Compliance Managers (Project 2008-09)

This recirculation ballot was conducted in error, and the results are void. Due to language changes by the drafting team, the interpretation should have been sent to a new initial ballot. A pre-ballot window will be initiated and announced in the next few days. Since this will be a new initial ballot, a new ballot pool will be formed during the pre-ballot window.

Project page: http://www.nerc.com/filez/standards/EOP-001-0_Interpretation_RECM.html

Ballot Criteria

Approval requires both:

- A 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
- 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.

Standards Development Process

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

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

Ballot Results	
Ballot Name:	Request for Interpretation - CIP-006-1a - US Army COE_in
Ballot Period:	1/5/2009 - 1/14/2009
Ballot Type:	Initial
Total # Votes:	206
Total Ballot Pool:	226
Quorum:	91.15 % The Quorum has been reached
Weighted Segment Vote:	97.39 %
Ballot Results:	The standard will proceed to recirculation ballot.

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	66	1	57	0.966	2	0.034	1	6
2 - Segment 2.	9	0.6	6	0.6	0	0	1	2
3 - Segment 3.	54	1	45	0.978	1	0.022	3	5
4 - Segment 4.	12	1	10	1	0	0	1	1
5 - Segment 5.	45	1	40	0.976	1	0.024	1	3
6 - Segment 6.	25	1	23	1	0	0	1	1
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	3	0.3	3	0.3	0	0	0	0
9 - Segment 9.	5	0.3	3	0.3	0	0	0	2
10 - Segment 10.	7	0.7	6	0.6	1	0.1	0	0
Totals	226	6.9	193	6.72	5	0.18	8	20

Individual Ballot Pool Results

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

1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Central Maine Power Company	Brian Conroy	Negative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Alan L Cooke	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	E.ON U.S. LLC	Larry Monday	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba		
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	Farmington Electric Utility System	Alan Glazner	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Florida Power & Light Co.	C. Martin Mennes	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	ITC Transmission	Elizabeth Howell	Affirmative	
1	Kansas City Power & Light Co.	Jim Useldinger	Affirmative	
1	Lincoln Electric System	Doug Bantam	Abstain	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	Minnesota Power, Inc.	Carol Gerou	Affirmative	
1	National Grid	Michael J Ranalli	Affirmative	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	PacifiCorp	Robert Williams	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
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	Sacramento Municipal Utility District	Dilip Mahendra	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Linda Brown		
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	
1	South Texas Electric Cooperative	Richard McLeon	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	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	Ronald P. Belval	Affirmative	
1	Westar Energy	Allen Klassen		
1	Western Area Power Administration	Robert Temple	Affirmative	
1	Xcel Energy, Inc.	Gregory L. Pieper	Affirmative	
2	Alberta Electric System Operator	Anita Lee		
2	British Columbia Transmission Corporation	Phil Park	Affirmative	
2	California ISO	David Hawkins	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Roy D. McCoy	Abstain	View
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Affirmative	

2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
3	Alabama Power Company	Robin Hurst	Affirmative	
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Negative	View
3	American Electric Power	Raj Rana	Affirmative	
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	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Tallahassee	Rusty S. Foster	Affirmative	
3	City Public Service of San Antonio	Edwin Les Barrow	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	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	Affirmative	View
3	Florida Power & Light Co.	W. R. Schoneck	Abstain	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W Pourciau		
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	Affirmative	
3	Lakeland Electric	Mace Hunter		
3	Lincoln Electric System	Bruce Merrill	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Ronald Dacombe	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	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	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	PacifiCorp	John Apperson	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. 1 of Chelan County	Kenneth R. Johnson	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange		
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	Southern California Edison Co.	David Schiada	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Wisconsin Public Service Corp.	James Maenner		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Chris Norton	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Florida Municipal Power Agency	Thomas Reedy	Abstain	
4	Georgia System Operations Corporation	Guy Andrews		
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Affirmative	
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	View
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Affirmative	

4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Alabama Electric Coop. Inc.	Tim Hattaway	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Black Hills Power	Pamela Pahl	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	City of Farmington	Clinton J Jacobs	Affirmative	
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Negative	
5	Conectiv Energy Supply, Inc.	Richard K. Douglass	Affirmative	
5	Constellation Generation Group	Michael F. Gildea	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Dairyland Power Coop.	Warren Schaefer	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Dynegy	Greg Mason	Affirmative	
5	East Kentucky Power Coop.	Stephen Ricker		
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	View
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	Lincoln Electric System	Dennis Florom	Abstain	
5	Louisville Gas and Electric Co.	Charlie Martin	Affirmative	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Oklahoma Gas and Electric Co.	Kim Morphis	Affirmative	
5	Orlando Utilities Commission	Richard Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp Energy	David Godfrey	Affirmative	
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	Reliant Energy Services	Thomas J. Bradish	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Southeastern Power Administration	Douglas Spencer	Affirmative	
5	Southern Company Services, Inc.	Roger D. Green		
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	
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	Black Hills Power	Larry Williamson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	William Franklin	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	View
6	Great River Energy	Donna Stephenson	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Louisville Gas and Electric Co.	Daryn Barker	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PacifiCorp	Gregory D Maxfield	Affirmative	
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	Salt River Project	Mike Hummel	Affirmative	

6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	
6	Western Area Power Administration - UGP Marketing	John Stonebarger	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	View
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
9	Oregon Public Utility Commission	Jerome Murray	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Negative	View
10	Midwest Reliability Organization	Larry Brusseau	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy Zito	Affirmative	View
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool	Charles H. Yeung	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on Initial Ballot — CIP-006-1a Requirement R4 for US Army (Project 2008-15)

Summary Consideration: Most balloters who submitted a comment were concerned that the existing standard does not require logging the time of egress and indicated this revision would improve the requirement. The drafting team agrees with these balloters and will share these comments with the drafting team working on revisions to the CIP-002-1 through CIP-009-1 standards.

Voter	Entity	Segment	Vote	Comment
Kirit S. Shah Mark Peters	Ameren Services Ameren Services	1 3	Negative Negative	We believe that logging and monitoring should be for both "in and Out".
Response: The interpretation can only address the requirement as currently written. Changes to the requirement, such as the inclusion of egress logging and monitoring, must be addressed via the standards development process. Several balloters expressed the same concern, and we will forward these comments to the drafting team that is working on revisions to the CIP standards.				
Robert Martinko Joanne Kathleen Borrell Kenneth Dresner Mark S Travaglianti Douglas Hohlbaugh	FirstEnergy Energy Delivery FirstEnergy Solutions FirstEnergy Solutions FirstEnergy Solutions Ohio Edison Company	1 3 5 6 4	Affirmative Affirmative Affirmative Affirmative Affirmative	FirstEnergy supports the interpretation of Requirement 4 of CIP-006. We offer the following suggestion regarding the proposed answer to the first question. In the answer, the team wrote "No, monitoring and logging of access are only required for ingress at this time." Although we agree that monitoring and logging is only required for ingress, the phrase "at this time" may imply that the requirement is not adequate as written and may need to be changed in the future. We feel that the interpretation should not imply the need for any changes to a requirement and suggest the team remove the phrase "at this time" from the interpretation.
Response: The use of "at this time" reflects that the interpretation can only address the requirement as currently written.				
Roy D. McCoy Kent Saathoff	Electric Reliability Council of Texas, Inc. Electric Reliability Council of	2 10	Abstain Negative	ERCOT recognizes that the CIP002-009 Version 1 Stds as written do NOT adequately address this area and we strongly recommend this matter be turned over to the Project CSO 706 Standards Drafting Team for resolution with their planned

Voter	Entity	Segment	Vote	Comment
	Texas, Inc.			Version 3 of the Cyber Security CIP Stds. These changes should be reviewed and approved consistent with NERC's formal Standards Development Process. ERCOT Security recognizes that CSO 706 STD team is currently focused on Version 2 changes with insufficient time to address this issue before the FERC deadline of July 2009. ERCOT recommends the SDT subsequently consider this matter (along with other FERC-directed changes) as part of the planned Version 3 of the Cyber Security Standards with changes to CIP-006-3/R4. ERCOT recommends that CIP-006/R4 be changed to include a requirement to log and monitor egress (as well as ingress) from protected areas containing Critical Assets and Critical Cyber Assets as defined in NERC CIP-002. Industry Best Security practices (ISO-27002 and NIST SP 800-53, Rev 2) specify that both ingress and egress monitoring should be performed for individuals entering and exiting areas which contain high-value, mission-critical cyber assets.
Response: Several balloters expressed the same concern, and we will forward these comments to the drafting team that is working on revisions to the CIP standards.				
Donald E. Nelson	Commonwealth of Massachusetts Department of Public Utilities	9	Affirmative	The revision of this standard should reconsider the logging of the total time an individual has spent in a cyber area by considering logging "departure" without creating deterrents to emergency exits and evacuations.
Response: Several balloters expressed the same concern, and we will forward these comments to the drafting team that is working on revisions to the CIP standards.				
Guy Zito	Northeast Power Coordinating Council, Inc.	10	Affirmative	NPCC would like future revisions to this standard to consider the implications of a requirement to track time spent within a critical cyber area to be recorded by logging the time a person leaves the area.
Response: Several balloters expressed the same concern, and we will forward these comments to the drafting team that is working on revisions to the CIP standards.				

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Recirculation Ballot Window Open
February 6–16, 2009

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

Interpretation of CIP-006-1a Requirement R4 for the US Army Corps of Engineers (Project 2008-15)

A recirculation ballot window is now open **until 8 p.m. EST on February 16, 2009** for a request for interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets. The US Army Corps of Engineers requested clarification for monitoring and logging physical access referenced in Requirement R4.

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2008-15_Interpretation_CIP-006-1a_US_Army_COE.html

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.

Standards Development Process

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Final Ballot Results

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

Interpretation of CIP-006-1a Requirement R4 for the US Army Corps of Engineers (Project 2008-15)

The ballot pool approved the interpretation. The interpretation will be submitted to the NERC Board of Trustees for adoption.

The recirculation ballot for Project 2008-15: Request for Interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets Requirement R4 ended February 16, 2009. The final ballot results are shown below. The Ballot Results Web page provides a link to the detailed results.

Quorum:	93.81%
Approval:	99.12%

Project Background

The US Army Corps of Engineers requested clarification for monitoring and logging physical access referenced in Requirement R4.

Project page: http://www.nerc.com/filez/standards/Project2008-15_Interpretation_CIP-006-1a_US_Army_COE.html

Ballot Criteria

Approval requires both:

- A 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
- 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.

Standards Development Process

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

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

Ballot Results	
Ballot Name:	Request for Interpretation - CIP-006-1a - US Army COE_rc
Ballot Period:	2/6/2009 - 2/16/2009
Ballot Type:	recirculation
Total # Votes:	212
Total Ballot Pool:	226
Quorum:	93.81 % The Quorum has been reached
Weighted Segment Vote:	99.12 %
Ballot Results:	The Standard has Passed

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	66	1	61	0.984	1	0.016	1	3
2 - Segment 2.	9	0.7	7	0.7	0	0	1	1
3 - Segment 3.	54	1	47	0.979	1	0.021	2	4
4 - Segment 4.	12	1	11	1	0	0	1	0
5 - Segment 5.	45	1	40	0.976	1	0.024	1	3
6 - Segment 6.	25	1	23	1	0	0	1	1
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	3	0.3	3	0.3	0	0	0	0
9 - Segment 9.	5	0.3	3	0.3	0	0	0	2
10 - Segment 10.	7	0.6	6	0.6	0	0	1	0
Totals	226	6.9	201	6.839	3	0.061	8	14

Individual Ballot Pool Results

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

1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Alan L Cooke	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	E.ON U.S. LLC	Larry Monday	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba		
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	Farmington Electric Utility System	Alan Glazner	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	C. Martin Mennes	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	ITC Transmission	Elizabeth Howell	Affirmative	
1	Kansas City Power & Light Co.	Jim Useldinger	Affirmative	
1	Lincoln Electric System	Doug Bantam	Abstain	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	Minnesota Power, Inc.	Carol Gerou	Affirmative	
1	National Grid	Michael J Ranalli	Affirmative	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	PacifiCorp	Robert Williams	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
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	Affirmative	
1	Sacramento Municipal Utility District	Dilip Mahendra	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Linda Brown		
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	
1	South Texas Electric Cooperative	Richard McLeon	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	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	Ronald P. Belval	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Robert Temple	Affirmative	
1	Xcel Energy, Inc.	Gregory L. Pieper	Affirmative	
2	Alberta Electric System Operator	Anita Lee	Affirmative	View
2	British Columbia Transmission Corporation	Phil Park	Affirmative	
2	California ISO	David Hawkins	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Roy D. McCoy	Abstain	View
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Affirmative	

2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
3	Alabama Power Company	Robin Hurst	Affirmative	
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Negative	View
3	American Electric Power	Raj Rana	Affirmative	
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	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Tallahassee	Rusty S. Foster	Affirmative	
3	City Public Service of San Antonio	Edwin Les Barrow	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	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	Affirmative	View
3	Florida Power & Light Co.	W. R. Schoneck	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W Pourciau		
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	Affirmative	
3	Lakeland Electric	Mace Hunter	Affirmative	
3	Lincoln Electric System	Bruce Merrill	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Ronald Dacombe	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	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	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	PacifiCorp	John Apperson	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. 1 of Chelan County	Kenneth R. Johnson	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange		
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	Southern California Edison Co.	David Schiada	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Wisconsin Public Service Corp.	James Maenner		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Chris Norton	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Florida Municipal Power Agency	Thomas Reedy	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Affirmative	
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	View
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Affirmative	

4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Alabama Electric Coop. Inc.	Tim Hattaway	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Black Hills Power	Pamela Pahl	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	City of Farmington	Clinton J Jacobs	Affirmative	
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Negative	
5	Conectiv Energy Supply, Inc.	Richard K. Douglass	Affirmative	
5	Constellation Generation Group	Michael F. Gildea	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Dairyland Power Coop.	Warren Schaefer	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Dynegy	Greg Mason	Affirmative	
5	East Kentucky Power Coop.	Stephen Ricker		
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	View
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	Lincoln Electric System	Dennis Florom	Abstain	
5	Louisville Gas and Electric Co.	Charlie Martin	Affirmative	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Oklahoma Gas and Electric Co.	Kim Morphis	Affirmative	
5	Orlando Utilities Commission	Richard Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp Energy	David Godfrey	Affirmative	
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	Reliant Energy Services	Thomas J. Bradish	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Southeastern Power Administration	Douglas Spencer	Affirmative	
5	Southern Company Services, Inc.	Roger D. Green		
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	
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	Black Hills Power	Larry Williamson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	William Franklin	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	View
6	Great River Energy	Donna Stephenson	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Louisville Gas and Electric Co.	Daryn Barker	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PacifiCorp	Gregory D Maxfield	Affirmative	
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	Salt River Project	Mike Hummel	Affirmative	

6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	
6	Western Area Power Administration - UGP Marketing	John Stonebarger	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	View
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
9	Oregon Public Utility Commission	Jerome Murray	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Abstain	View
10	Midwest Reliability Organization	Larry Brusseau	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy Zito	Affirmative	View
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool	Charles H. Yeung	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

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

Exhibit D

Interpretation Development Team Rosters

Interpretation — CIP-006-1a, R1 — SCE&G Drafting Team
(Project 2007-27)

Paul McClay Manager of Information Security	Tampa Electric Co. P.O. Box 111 Tampa, FL 33601	(813) 225-5287 (813) 225-5302 Fx pfmcclay@tecoenergy.com
Patrick Miller	PacifiCorp	Patrick.Miller@PacifiCorp.com
Robert Sypult	SCE	robert.sypult@sce.com
David L. Norton Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue - MS: L-MOB-17A New Orleans, LA 70113	(504) 576-5469 (504) 576-5123 Fx dnorto1@entergy.com
David R. Ambrose SCADA System Manager	Western Area Power Administration - Rocky Mountain Region 5555 E. Crossroads Blvd. Loveland, CO 80538	(970) 461-7354 (970) 461-7213 Fx ambrose@wapa.gov
George Miserendino	Triton Security Solutions, Inc. 4959 138th Circle W. Apple Valley, MN 55124-9229	(952) 423-3457 (952) 322-2505 Fx george@tritonsecsol.com
Harry Tom NERC Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx harry.tom@nerc.net
Scott Mix	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx scott.mix@nerc.net

Interpretation — CIP-006-1a, R4 — US Army Corp. of Engineers Drafting Team (Project 2008-15)

Larry Bugh — Chairman Chief Security Officer	ReliabilityFirst Corporation 320 Springside Drive — Suite 300 Akron, Ohio 44333	(330) 247-3046 (330) 456-3648 Fx larry.bugh@rfirst.org
Jonathan Bransky IT Security Manager	Public Service Enterprise Group Incorporated 80 Park Plaza — T-16 Newark, New Jersey 07102	(973) 430-6294 jonathan.bransky@pseg.com
David Dunn	Independent Electricity System Operator	(905) 855-6286 david.dunn@ieso.ca
Mark A. Engels Director — IT Risk Management	Dominion Virginia Power P.O. Box 26666 Richmond, Virginia 23261	(804) 775-5263 (804) 771-3067 Fx mark.engels@dom.com
Chris Humphreys	Texas Regional Entity	(512) 275-7440 christopher.humphreys@ texasre.org
Michael Mertz	Southern California Edison Technology & Risk Management	(626)543-6104 Michael.Mertz@sce.com
James W. Sample Manager of Information Security	California ISO 151 Blue Ravine Road Folsom, California 95630	(916) 608-5891 (916) 351-2373 Fx jsample@caiso.com
William Souza	PJM Interconnection, L.L.C.	(610) 666-2237 souzaw@pjm.com
Al Calafiore NERC Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx al.calafiore@nerc.net
Scott Mix NERC Manager of Situation Awareness and Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx scott.mix@nerc.net