May 23, 2012

VIA ELECTRONIC FILING

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

Re: *North American Electric Reliability Corporation*
Docket No._____

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits this petition in accordance with Section 215(d)(1) of the Federal Power Act ("FPA") and Part 39.5 of the Federal Energy Regulatory Commission's ("FERC" or "the Commission") regulations seeking approval of an interpretation to Requirement R1.1 to Reliability Standard CIP-006-4,[1] as set forth in **Exhibit A** to this petition, to become effective concurrent with the date of a FERC Order approving this petition.

This interpretation was approved by the NERC Board of Trustees on February 9, 2012. Upon approval, the standard will be referred to as CIP-006-3d or CIP-006-4d, whichever version of the standard is in effect at the time of FERC approval.[2]NERC's petition consists of the following:

[1] This interpretation applies to Versions 1, 2, 3, and 4 of the CIP-006 standard. For purposes of this filing, the standard will be referred to as CIP-006-4.
[2] At the time this request for interpretation was submitted to NERC, Version 1 of the CIP standards was in effect. The request was therefore processed referencing CIP-006-1. Subsequently, Versions 2, 3 and 4 of the CIP standards were approved by FERC. However, the changes in Versions 2, 3, and 4, relative to Version 1 of CIP-006, are not material to the substance of the interpretation request. Given that Version 3

- This transmittal letter;
- A table of contents for the filing;
- A narrative description explaining the interpretation and how it meets the reliability goal of the standard;
- Interpretation of Requirement R1.1 of CIP-006-4 (**Exhibit A**);
- Reliability Standard CIP-006-3d, that includes the appended interpretations of Requirement R1.1, submitted for approval (**Exhibit B1**);
- Reliability Standard CIP-006-4d, that includes the appended interpretations of Requirement R1.1, submitted for approval (**Exhibit B2**);
- Consideration of Comments for interpretations to Requirements R1.1 of CIP-006-4 (**Exhibit C**);
- The complete development record of the interpretation Requirement R1.1 of CIP-006-4 (**Exhibit D**); and
- A roster of the interpretation drafting team for the interpretations of Requirement R1.1 of CIP-006-4 **(Exhibit E**).

For the reasons stated above and in this petition, NERC respectfully requests that the Commission approve the interpretation presented herein for approval.

Respectfully submitted,

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation

---

is currently-effective, and Version 4 will become effective on April 1, 2014, NERC will append the requested interpretation to Version 3 or Version 4 of the CIP-006 standard, whichever is in effect at the time of FERC approval of this interpretation, in lieu of Version 1. *See Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (September 30, 2009); *Order on Compliance*, 130 FERC ¶ 61,271 (2010) (March 31, 2010); *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (April 19, 2012).

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**) Docket No. RM-__-000)**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF INTERPRETATION TO RELIABILITY STANDARD CIP-006 – CYBER SECURITY — PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

May 23, 2012

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[3] hereby requests the Federal Energy Regulatory Commission ("FERC" or "Commission") to approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[4] and Section 39.5 of FERC's Regulations,[5] a proposed interpretation to Reliability Standard CIP-006-4[6] — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, to become effective concurrent with the date of a FERC Order approving this petition.[7]

No modification to the language contained in this specific requirement is being proposed through the interpretation. The NERC Board of Trustees approved the interpretation to CIP-006-4 on February 9, 2012. NERC requests that FERC approve the interpretation to Reliability Standard CIP-006-3 or CIP-006-4, to cover the different versions of the standard as they currently exist or become effective, and make the interpretation effective immediately upon approval in accordance with FERC's procedures.

Upon Commission approval of the interpretation, the standard will be referred to as CIP-006-3d or CIP-006-4d — Cyber Security — Physical Security of Critical Cyber Assets, whichever version of the standard is in effect at the time of FERC approval. For ease of reference, the interpretation will be referred to as CIP-006-4d in this filing.

---

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

[4] 16 U.S.C. 824o (2006).

[5] 18 C.F.R. § 39.5 (2011).

[6] The proposed interpretation applies to versions 1, 2, 3, and 4 of the standard. For purposes of this filing, the standard will be referred to as CIP-006-4.

[7] Capitalized terms not otherwise defined, shall have the meaning set forth in the *NERC Glossary of Terms Used in NERC Reliability Standards*, available at: http://www.nerc.com/files/Glossary_of_Terms.pdf.

Exhibit A to this petition sets forth the interpretation of Requirement R1.1 to CIP-006-4. **Exhibit B1** to this petition contains proposed Reliability Standard CIP-006-3d, which includes the appended interpretation of Requirement R1.1. **Exhibit B2** to this petition contains proposed Reliability Standard CIP-006-4d, which includes the appended interpretation of Requirement R1.1. **Exhibit C** contains the drafting team's consideration of industry comments for the interpretation to Requirement R1.1. **Exhibit D** contains the complete development history of the Interpretation of Requirement R1.1 of CIP-006-4. **Exhibit E** contains the roster of the interpretation drafting team that drafted the interpretation of Requirement R1.1.

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

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[8]

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
david.cook@nerc.net

Holly A. Hawkins*
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Willie L. Phillips*
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

III. BACKGROUND

a. Regulatory Framework

By enacting the Energy Policy Act of 2005,[9] Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the bulk power system, and with the duties of certifying an electric reliability organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. Section 215 states that all users, owners and operators of the bulk power system in the United States will be subject to FERC-approved Reliability Standards.

b. Basis for Approval of Proposed Reliability Standard Interpretation

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

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

The proposed Reliability Standard contains an interpretation of a requirement within a Commission-approved Reliability Standard, but does not represent a new or modified Reliability Standard. The proposed Reliability Standard interpretation provides additional clarity with regard to the intent of the Reliability Standard. Therefore, NERC requests that the Commission approve the proposed interpretation.

c. Reliability Standards Development Procedure and Interpretation

All persons who are directly or materially affected by the reliability of the North American bulk power system are permitted to request an interpretation of a Reliability Standard, as discussed in NERC's *Standard Processes Manual*,[10] which is incorporated into the NERC Rules of Procedure as Appendix 3A.

The process for responding to a valid request for interpretation requires NERC to assemble a team with the relevant expertise to address the interpretation request. The interpretation drafting team is then required to draft a response to the request for interpretation and then present that response for industry ballot. If approved by the ballot pool and the NERC Board of Trustees, the interpretation is appended to the Reliability Standard and filed for approval with FERC and applicable governmental authorities in Canada. And once the affected Reliability Standard undergoes its next substantive revision, the interpretation will be incorporated into the Reliability Standard, as appropriate.

[10] FERC approved the new *Standard Processes Manual* in the *Order Approving Petition and Directing Compliance Filing*, (132 FERC ¶ 61,200 (2010), which replaced NERC's *Reliability Standards Development Procedure Version 7* in its entirety. NERC developed these interpretations in accordance with the *Reliability Standards Development Procedure Version 7* until the *Standard Processes Manual* was approved on September 3, 2010. NERC's *Reliability Standards Development Procedure* is available at: http://www.nerc.com/fileUploads/File/Standards/RSDP_V6_1_12Mar07.pdf. The Standard Processes Manual is available at: http://www.nerc.com/files/Appendix_3A_Standard_Processes_Manual_20100903.pdf.

The standing CIP interpretation drafting team was appointed to develop the response to the instant request for interpretation regarding Requirement R1.1 of CIP-006-4. The proposed interpretation included as **Exhibit A** was approved by the ballot pool on December 19, 2011, with a ballot pool quorum of 88.02 percent and weighted segment approval of 96.04 percent. It was approved by the NERC Board of Trustees on February 9, 2012.

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

The Commission approved Reliability Standard CIP-006-1 in Order No. 706,[11] Reliability Standard CIP-006-2 in the September 30, 2009 Order,[12] Reliability Standard CIP-006-3 in the March 31, 2010 Order, [13] and Reliability Standard CIP-006-4 in Order No. 761.[14]

This filing includes the proposed Reliability Standard CIP-006-3d that contains the appended interpretation in **Exhibit B1**, and proposed Reliability Standard CIP-006-4d that contains the appended interpretation in **Exhibit B2**. In Section IV(a), below, NERC summarizes the justification for the proposed interpretation of Requirements R1.1 of the standard, and explains the development of the interpretation. Section IV(b) describes the stakeholder ballot results and provides an explanation of how stakeholder comments were considered and addressed by the interpretation drafting team assembled to develop the interpretation. The interpretation drafting team's considerations of comments for the

[11] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, at PP 24 and 581 (2008), *order on clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, 126 FERC ¶ 61,229 (2009).
[12] *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (September 30, 2009).
[13] *Order on Compliance*, 130 FERC ¶ 61,271(March 31, 2010).
[14] *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (April 19, 2012).

interpretation is contained in **Exhibit C**. The complete development record for the interpretation, set forth in **Exhibit D,** 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 E** contains the roster of the team members who developed the proposed interpretation.

a. Justification for Approval of Interpretation

The stated purpose of Reliability Standard CIP-006-4 — Cyber Security — Physical Security of Critical Cyber Assets is to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Requirement R1 of CIP-006-4 provides:

> **R1.** Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > **R1.1.** All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

In April 2008, Progress Energy requested an interpretation of Requirement R1 of CIP-006-1.[15] Specifically, Progress Energy sought clarification with respect to the following language in CIP-006-4, Requirement R1.1:

[15] At the time this request for interpretation was submitted to NERC, Version 1 of the CIP standards was in effect. The request was therefore processed referencing CIP-006-1. Subsequently, Versions 2, 3 and 4 of the CIP standards were approved by FERC. However, the changes in Versions 2, 3, and 4, relative to Version 1 of CIP-006, are not material to the substance of the interpretation request. Given that Version 3 is currently-effective, and Version 4 will become effective on April 1, 2014, NERC will append the requested interpretation to Version 3 or Version 4 of the CIP-006 standard, whichever is in effect at the time of FERC approval of this interpretation, in lieu of Version 1. *See Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291

Request:

Progress Energy requests a formal interpretation of CIP-006-1Requirement R1.1.

In CIP-006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

> *R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*
> *R3.2. The Cyber Asset uses a routable protocol within a control center; or,*
> *R3.3. The Cyber Asset is dial-up accessible.*

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

In response to Progress Energy's interpretation request, the interpretation drafting team developed, and the industry stakeholders approved, the following interpretation:

(September 30, 2009); *Order on Compliance,* 130 FERC ¶ 61,271 (2010) (March 31, 2010); *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (April 19, 2012).

Response:

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset." The definition of "Cyber Asset" in the NERC Glossary of Terms Used in Reliability Standards includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 1. The interpretation in CIP-006-3c, appendix 1, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

The interpretation of Requirement R1.1 of CIP-006-4 is consistent with the stated purpose of the Reliability Standard, which is to ensure that Critical Cyber Assets are protected. As part of a physical security program, the standard requires the creation and maintenance of a Physical Security Plan that addresses protection of Cyber Assets within a Physical Security Perimeter. In this context, the interpretation discusses the distinction between a Cyber Asset and underlying components of Cyber Assets that are not themselves classified Cyber Assets. Since the requirement only applies to a Cyber Asset, and wiring is not a Cyber Asset, the requirement does not apply to wiring. Accordingly, the interpretation clarifies that Requirement R1.1 of CIP-006-4 does not apply to wiring.

In finding that wiring is not a Cyber Asset, and thus not subject to the requirement, the interpretation drafting team determined that the definition of Cyber Asset in the *Glossary of Terms Used in NERC Reliability Standards* does not include communication mediums (*i.e.*, wiring).[16]

[16] *NERC Glossary of Terms Used in NERC Reliability Standards*, at p. 14, available at: http://www.nerc.com/files/Glossary_of_Terms.pdf.

A "communication network," which is included in the definition of a Cyber Asset, is typically a set of devices and a population of data, but not the wires or any other supporting component. For example, as noted by members of the interpretation drafting team, a "communication network" uses electricity and power cables. Although electricity and power cables are essential components of a communication network, they are not classified as Cyber Assets. Moreover, while the term "data" is included in the definition of Cyber Asset, the use of wiring to transmit data does not automatically transform wiring into a Cyber Asset.[17] Even so, NERC notes that CIP-005 requires the identification and protection of the ESP inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

Assuming *arguendo* that "wiring" is a Cyber Asset, wiring would then be subject to all Reliability Standards that apply to Cyber Assets. Such a reading of NERC's Cyber Asset definition would lead to an unintended application of the CIP standards and the wasting of limited industry resources. Therefore, the proposed interpretation is consistent with the definition of Cyber Asset and the Reliability Standard's purpose.[18]

b. Summary of the Reliability Standard Development Proceedings

NERC presented the interpretation of CIP-006-4, Requirement R1.1 for a first initial ballot from August 7, 2008, through August 16, 2008, and achieved a quorum of 88.18 percent with a weighted affirmative approval of 21.52 percent. There were 142

[17] *Id*.
[18] This interpretation also clarifies a separate question from a previously-approved interpretation to the same requirement. The proposed interpretation is limited to whether the requirement applies at all (in this case, to "wiring"). The previously approved interpretation assumes that the standard applies, and then provides clarity on the "alternative measures" component of CIP-006-4, Requirement R1.1, after determining that a fully enclosed six-wall border cannot be established around the applicable Cyber Asset.

negative ballots submitted in the initial ballot, and 97 of those ballots included a comment, which initiated the need for another initial ballot.

A second draft interpretation was developed and posted for initial ballot from November 30, 2009, to October 12, 2009. Stakeholders supported the draft interpretation, which achieved a quorum of 79.92 percent with a weighted affirmative approval of 74.47 percent. There were 46 negative ballots submitted in the second initial ballot, and 30 of those ballots included a comment; however, work on the interpretation was delayed based on reprioritization of the total standards workload in accordance with guidance from the NERC Board of Trustees issued November 2009.

In April 2011, the Standards Committee approved and issued the *NERC Guidelines for Interpretation Drafting Teams*, and the Standards Committee directed that work resume on the interpretation.[19] A project team assembled from members of the CIP interpretation drafting team reviewed and responded to the comments received during the last successive ballot and made revisions to the interpretation. The interpretation drafting team ultimately determined that the second draft interpretation did not conform to the new guidelines. Consequently, the interpretation drafting team revised the interpretation to be limited to the question asked: whether CIP-006-1, Requirement R1.1, applies to the aspects of wiring that comprises the ESP.

An updated draft of the interpretation was posted for successive ballot on October 12, 2011, with the ballot occurring from November 11 through November 21, 2011. The ballot achieved a 95.99% approval, with a quorum of 83.53%. There were 9 negative

[19] *NERC Guidelines for Interpretation Drafting Teams*, available at: http://www.nerc.com/files/Guidelines_for_Interpretation_Drafting_Teams_Approved_April_2011.pdf.

ballots submitted in the successive ballot, and 5 of those ballots included a comment, which initiated the need for a recirculation ballot.

A recirculation ballot was held from December 9, 2011 to December 19, 2011, and the interpretation was approved by stakeholders, achieving 96.04 percent approval with a quorum of 88.02 percent.

As demonstrated in the summary of comments presented below, some commenters noted disagreement with the standard drafting team's interpretation that wiring is not a Cyber Asset. Some balloters commented on more than one issue. More specifically, the reasons cited for the negative ballots included the following:

- 1 balloter did not believe the Request for Interpretation was clear enough to formulate an interpretation and that Progress Energy should have been afforded an opportunity to reformulate its question. The interpretation drafting team and majority of balloters agree, however, that the interpretation was able to provide clarity to the meaning of the requirement through its analysis.
- 1 balloter indicated that the interpretation did not provide enough clarity and should be addressed in future versions of the standard. The interpretation drafting team and balloters agree, however, that the interpretation was able to provide clarity to the meaning of the requirement through its analysis.
- 1 balloter indicated that the interpretation is flawed because it defines wiring as a Cyber Asset and expands the requirement, and that the "six-wall" border issue should not be addressed. It is presumed that this

balloter perhaps read an earlier draft of the interpretation when commenting.

- 1 balloter noted that a wire is the transport medium for the data, and data is a Cyber Asset. CIP-006-3, R1.1, requires data to be protected; to protect the data, the wire must also be protected. The interpretation drafting team determined that wire is an underlying component of a Cyber Asset and therefore not a Cyber Asset), which is consistent with CIP-006-3c, R1.1's requirement to protect data.
- 1 balloter noted that wiring is an essential component of the hardware comprising a network, further supporting the need to protect the wiring. The interpretation drafting team noted that it is outside the scope of the language of the definition of "Cyber Asset," and CIP-006-4c, R1.1's application is limited to Cyber Assets.

c. Future Action

Reliability Standard CIP-006-4c was approved by Commission on April 19, 2012, in Docket No. RM11-11-000. Upon Commission approval of the requested interpretation, the interpretation shall remain in effect until such time as the interpretation can be incorporated into a future revision of the standard.

V. CONCLUSION

NERC respectfully requests that FERC approve the interpretation to FERC-approved Reliability Standard CIP-006-4— Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, as set out in **Exhibit A**, in accordance with Section 215(d)(1) of the FPA and Part 39.5 of FERC's regulations. NERC requests that this interpretation be made effective immediately upon issuance of FERC's order in this proceeding.

Respectfully submitted,

/s/ *Willie L. Phillips*

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 23rd day of May, 2012.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation

Exhibit A

Interpretation of Requirement R1.1 of CIP-006-4

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets
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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."
The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 1. The interpretation in CIP-006-3c, appendix 1, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

Exhibit B1

Reliability Standard CIP-006-3, that includes the appended interpretation of Requirement R1.1, submitted for approval

A. Introduction

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

2. Number: CIP-006-3d

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

4. Applicability:

4.1. Within the text of Standard CIP-006-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-3:

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

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

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

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

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

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

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized

access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -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.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24, 2011	Adopted by NERC Board of Trustees	
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4.	

		Updated version number from -3/-4 to -3c/-4c.	
3d/4d	February 9, 2012	Interpretation of R1.1 adopted by NERC Board of Trustees	Project 2008-10

Appendix 1

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

Appendix 2

Interpretation of Requirement R1.1.

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

Interpretation:

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

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

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

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

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

1.4. Additional Compliance Information

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

Appendix 3

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

Request:

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

Interpretation:

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

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

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

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

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

Appendix 4[1]

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:

Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- *R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*
- *R3.2. The Cyber Asset uses a routable protocol within a control center; or,*
- *R3.3. The Cyber Asset is dial-up accessible.*

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets

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:

[1] When the request for interpretation was made, it was for a previous version of the standard. Although the interpretation references a previous version of the standard, because it is still applicable in this case, it is appended to this version of the standard.

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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."

The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 1. The interpretation in CIP-006-3c, appendix 1, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

Exhibit B2

Reliability Standard CIP-006-4, that includes the appended interpretation of Requirement R1.1, submitted for approval

A. Introduction

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

2. Number: CIP-006-4d

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. 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-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

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-008-4. 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-008-4.

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

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

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep 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-006-4 for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -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.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31,	FERC Order issued approving CIP-006-3	

	2010		
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24, 2011	Adopted by NERC Board of Trustees	
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	
3d/4d	February 9, 2012	Interpretation of R1.1 adopted by NERC Board of Trustees	Project 2008-10

Appendix 1

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

Appendix 2

Interpretation of Requirement R1.1.

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

Interpretation:

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

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

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

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

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

1.4. Additional Compliance Information

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

Appendix 3

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

Request:

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

Interpretation:

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

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

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

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

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

Appendix 4[1]

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:

Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- *R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*
- *R3.2. The Cyber Asset uses a routable protocol within a control center; or,*
- *R3.3. The Cyber Asset is dial-up accessible.*

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets

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:

[1] When the request for interpretation was made, it was for a previous version of the standard. Although the interpretation references a previous version of the standard, because it is still applicable in this case, it is appended to this version of the standard.

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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter***.** *Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."

The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 1. The interpretation in CIP-006-3c, appendix 1, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

Exhibit C

Consideration of Comments for interpretation to Requirement R1.1 of CIP-006-4

Project 2008-10
Interpretation - CIP-006 - Cyber Security — Physical Security of Cyber Security Assets

Registered Ballot Body

Related Files

Status:
A recirculation ballot of the interpretation ended on December 19, 2011. The interpretation was approved by the ballot pool with a quorum of 88.02% and weighted segment approval of 96.04%. The interpretation will be presented to the NERC Board of Trustees for adoption in February 2012 and if adopted, filed with regulators for approval.

Background:
Progress Energy asked if Electronic Security Perimeter wiring external to a Physical Security Perimeter must be protected within a six-wall boundary.

Draft	Action	Dates	Results	Consideration of Comments
Interpretation of CIP-006-x R1 for Progress Energy Draft Interpretation Clean | Redline to Last Posting **Supporting Materials:** CIP-006-3C	Recirculation Ballot Info>> Vote>>	12/09/11 - 12/19/11 (closed)	Summary>> Full Record>>	
Interpretation of CIP-006-x R1 for Progress Energy Draft Interpretation Clean | Redline to Last Posting **Supporting Materials:** Unofficial Comment Form CIP-006-3C	Successive Ballot Vote>>	11/11/11 - 11/21/11 (closed)	Summary>> Full Record>>	
	Formal Comment Period Info>>	10/12/11 - 11/21/11 (closed)		Consideration of Comments**(3)**

	Submit Comments>>			
	Join Ballot Pool>>	10/12/11 - 11/10/11 (closed)		
Progress Energy CIP-006-1, Requirement R1.1 - Automatic Generation Control Revised Interpretation Request for Interpretation	Initial Ballot Info>> | Vote>>	09/30/09 – 10/12/09 (closed)	Summary>> Full Record>>	Consideration of Comments**(2)**
	Pre-ballot Review Info>> | Join>>	08/31/09 – 09/30/09 (closed)		
Progress Energy CIP-006-1, Requirement R1.1 - Automatic Generation Control Interpretation Request for Interpretation	Initial Ballot Vote>>	08/07/08 – 08/16/08 (closed)	Full Record>>	Consideration of Comments**(1)**
	Pre-ballot Window Info>> | Join>>	07/08/08 – 08/07/08 (closed)		
To download a file click on the file using your right mouse button, then save it to your computer in a directory of your choice.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on Initial Ballot — CIP-006-1 — Progress Energy Request for Interpretation (Project 2008-10)

Summary Consideration: There are five themes that emerged from the industry comments:

1) Wiring does not rely upon or utilize a routable protocol and thus cannot be a cyber asset any more than a power cable is. The NERC definition of cyber asset does not include the language "including the wiring that comprises the physical media supporting the network."

Response: The interpretation response team has reviewed its response and considers the wiring to be a component of the communication network, which is a cyber asset, as defined in the NERC Glossary. As such, the network wiring needs to be protected.

2) This is far too important to resolve via an interpretation. This needs to be addressed in the revisions to the CIP standards and subject to the full stakeholder process.

Response: We agree that this is an important issue, and it will be considered as part of the standards' revision in the Cyber Security Order 706 (CSO706) project (Project 2008-06). However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this request for interpretation (RFI) from Progress Energy.

3) The interpretation exceeds the process rules by changing the requirements of standard, adds concepts not consistent with other NERC guidance, speculates on the intent of the standard, and adds confusion and ambiguity with respect to compliance. It also opens the door for other non-physical "alternatives" to compliance with the requirements of CIP-006.

Response: While the drafting team disagrees it altered any requirements to the standard via the interpretation, the team acknowledges a lack of clarity regarding alternative measures. In drafting the revised interpretation, the team interprets the phrase "alternative measures" to include use of combined/complementary physical and logical approaches to achieve the same or better protection for Electronic Security Perimeter (ESP) wiring that is external to the Physical Security Perimeter (PSP).

4) The wire is not within the ESP; therefore it does not need to be protected. The wire is nothing more than a communication link specifically excluded by CIP-005, R1.3.

Response: The request clearly asked about wiring within an ESP.

5) The cost (dollars, time) to protect wiring in a campus setting far exceeds the benefit derived by doing so. The challenges of having to comply with all of the CIP-006 requirements are an impossible and unreasonable task. The decision to protect wiring should be based upon a proper risk determination process.

Response: The interpretation response team attempted to offer alternative methods for compliance without undue financial burden in the initial interpretation response. In drafting the revised interpretation, the team interprets the phrase "alternative measures" to include use of combined/complementary physical and logical approaches to achieve the same or better protection.

Entity	Segment	Vote	Comment
Allegheny Power	1	Negative	Allegheny Energy is concerned with the SAR drafting team interpretation that wiring within an ESP be considered a Cyber Asset or Critical Cyber Asset. Allegheny Energy agrees that the wiring (and information

Entity	Segment	Vote	Comment
			transmitted by such wiring) within an ESP needs to be protected; however, Allegheny Energy does not agree that the wiring needs to be classified and protected as a defined cyber asset. NERC defines cyber assets as programmable electronic devices and communication networks including hardware, software, and data and does not include the language “including the wiring that comprises the physical media supporting the network”. Allegheny Energy believes the best method to determine protection measures for the wiring (and information transmitted by such wiring) is to create a holistic approach to communication network and data communication link protection through the Standards process that specifically addresses these issues. This new Standard could address communication network and data communication link security issues, including copper cabling, fiber optic cabling, and wireless implementations. By the interpretation stating that network wiring is a cyber asset or potentially a critical cyber asset in an effort to physically secure the wiring, this statement would additionally impose all of the requirements of the CIP standard that are applicable to cyber assets and in essence make entities non-compliant since many requirements cannot be accomplished for wiring.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. For ESP wiring that is external to the PSP: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or monitoring to detect unauthorized access or physical tampering. The RFI response drafting team agrees that this is an important issue and it will be considered as part of the standards’ revision in the Cyber Security Order 706 (CSO706) project.			
Ameren Services Company	1	Negative	We do not agree with this interpretation. We feel that the language in the first sentence of the response, "including the wiring that comprises the physical media supporting the network," could be viewed to include aspects that are not covered in the CIP 002 - 009. Broad interpretation of the response would significantly impact the compliance burden. In addition, CIP 006 R1.1 states: "Where a completely enclosed (six-wall) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." This interpretation does not make it clear whether or not that part of the CIP-006 requirement 006 is still valid, and seems to supersede the CIP standard in this regard.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within			

Entity	Segment	Vote	Comment
an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
American Electric Power	1	Negative	Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue and it is presently being considered as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A methodology for determining the appropriate protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Associated Electric	1	Negative	Wiring meets none of the requirements of CIP-002-R3, the wiring does not communicate itself with anything, it is merely a communications conduit or channel, therefore the standard does not apply to it anymore than it

Entity	Segment	Vote	Comment
Cooperative, Inc.			would apply to the ac power wiring. While it is appropriate to protect access to all wiring inside the ESP, I do not believe that the intent of the standard is to consider wiring a CCA and subject it to all of the CIP requirements, many of which can not even be implemented or do not apply. These points were presented very well (and I am in complete agreement with) in the document by Mr. Tim Conway of NiSource, “Wiring as a CCA”.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Brazos Electric Power Cooperative, Inc.	1	Negative	Further clarity should be added to the last sentence to address the interpretation request as follows: Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures as it extends from the ESP up to the Physical Security Perimeter. Then there is the question about what is defined as "tampering".
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering. The RFI response drafting team views tampering to include, but is not limited to, unauthorized access, disruption, or alteration.			
Consolidated Edison Co. of New York	1	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.

Entity	Segment	Vote	Comment
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
FirstEnergy Energy Delivery	1	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that "Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The communication assets excluded from the standards are the Cyber Assets associated with communication networks and data communication links between			

Entity	Segment	Vote	Comment
discrete ESPs. There is no explicit reference within the standards to third-party communications. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Hydro One Networks, Inc.	1	Negative	Hydro One Networks Inc. is casting a Negative vote with the following comment: The interpretation is not clear and may modify the intention of the Standard. It needs more work. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter," which must be protected. While the wires connecting two ESPs need to be protected it should not make one PSP of both. Appropriate conduit or similar protection as appropriate should be acceptable.
Response: The equipment configuration described in this comment wherein two physically separate Cyber Assets that are individually classified as having its own ESP would indeed not require physical access protection for the interconnecting wiring. However, the situation as described by the requestor is different. The configuration indicated by the requestor involves physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Manitoba Hydro	1	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that “the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network.” It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised RFI response. The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the			

Entity	Segment	Vote	Comment
drafting team disagrees with removal of the term communication network in the RFI response as it is already referenced in the NERC Glossary definition of a Critical Cyber Asset.			
National Grid	1	Negative	The interpretation is not clear and may modify the intention of the Standard. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures for ESP wiring that is external to the PSP may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
New Brunswick Power Transmission Corporation	1	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "…all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Orange and Rockland Utilities, Inc.	1	Negative	Orange and Rockland cannot support CIP-006 R1.1 and requests further clarification of "alternative protection measures" encompassing the wiring that comprises the "physical media" supporting the network.
Response: The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures for ESP wiring that is external to the PSP may include, but are not			

Entity	Segment	Vote	Comment
limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Pacific Gas and Electric Company	1	Negative	As written the interpretation is too broad. The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within the pertinent parts of a given facility or campus.
Response: The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures for ESP wiring that is external to the PSP may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
PacifiCorp	1	Negative	"The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets "alternative measures" for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering. The drafting team believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected not to include such language.			
Potomac Electric	1	Negative	Pepco is a subsidiary of PHI. PHI feels that the interpretation is not clear and the response itself is subject to interpretation. This lack of clarity is the basis for PHI's rejection. PHI also believes that communication systems

Entity	Segment	Vote	Comment
Power Co.			should be protected. The Answer to Question 11 of the FAQ associated with these standards states that communication systems are not covered by these standards.

Response:

The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The asset owner is encouraged to reconsider the design of a communication network that extends the ESP across third-party communications systems and networks.

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

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

Question 11 of the FAQ for standard CIP-002-1 – Cyber Security – Critical Cyber Assets (reproduced below) refers to Section A 4.2.2 regarding the exclusion of Cyber Assets associated with communication networks and data communication links between discrete ESPs. Communications within the ESP are covered by these standards.

CIP-006-1 The asset owner is encouraged to reconsider the design of a communication network that extends the ESP across third-party communications systems and networks.

11. FAQ - Question: *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?*

Answer: Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset.

PP&L, Inc.	1	Negative	The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.

Response:

The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.

Entity	Segment	Vote	Comment
Puget Sound Energy, Inc.	1	Negative	Definition of Cyber Asset: We do not believe the existing definition of "Cyber Asset" should include wiring. From the most recent (February 12, 2008) NERC "Glossary of Terms Used in Reliability Standards": "Cyber Assets - Programmable electronic devices and communication networks including hardware, software, and data." Wires are not programmable, are not software, and are not data. While they are physical media, it is highly questionable if they could be considered hardware as our understanding is that hardware devices are what software runs on. If we were to extend the definition to include a wire strictly because it carries data, at what point do we consider a telephone pole a Cyber Asset because it carries wires which carry data? If the definition does include wiring, how then do wireless communications media fit into the definition in the context of physical protection of Cyber Assets? Wireless is neither hardware, software, or data and, with regards to this interpretation, physical protection of airborne electrons is not practical/possible with today's technology. Alternative Protective Measures: As most facilities which house Critical Cyber Assets were constructed prior to the CIP standard adoption by FERC, many such facilities have a common wiring infrastructure for both Critical Cyber Assets and assets that are not in scope for CIP compliance. We believe it is unreasonable to require every wire be traced and extracted from common conduit, cable bundles, or other common pathway for the purposes of re-enclosing them in a CIP-specific conduit or other “six-wall” perimeter. The very act of performing this work will introduce an increased reliability risk. If wiring is to be included in the definition of Cyber Asset, we feel that a “completely enclosed (“six-wall”) border” cannot be established for most wiring infrastructures given the above. Therefore, the "alternative measures to control physical access to the Critical Cyber Assets" phrase from CIP-006 R1.1 must be used. The definition for Critical Cyber Assets require that a Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, the Cyber Asset uses a routable protocol within a control center; or, the Cyber Asset is dial-up accessible, and wiring has no such attributes. Given that CIP-006 R1.1 talks about both Cyber Assets and Critical Cyber Assets, can the interpretation team comment on the above? We would also like clarification on whether "alternative protective measures" includes situations that only deploy purely logical controls of data transiting the wire. As the interpretation team has stated, “The intent is to protect the data transmitted over the network within the ESP”, would an ESP that spans an entity’s entire infrastructure and only employs logical “alternative protective measures”, be an acceptable response to this interpretation? Summary: We commend the interpretation team for wanting to address data in motion, but the appropriate venue to address this issue is NERC Project 2008-06 as CIP-006 R1.1 prescribes requirements for physical protection of Cyber Assets (or just Critical Cyber Assets when a “six-wall” perimeter cannot be established) within an ESP. Additionally, based on our assessment of the term Cyber Asset, we believe requirements to protect communications media are beyond the scope of the existing CIPs. Outstanding RFI How does the Project 2008-10 interpretation for Progress Energy relate to the previous interpretation request (below) from October 10, 2007 by Puget Sound Energy? --- 1) We are requesting an interpretation of the term “externally connected” as used in 005.R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s) We request an interpretation which allows encrypted connections over frame relay within a single ESP. Note in the diagram above the routers are not considered “access points” to the ESP, but rather are contained within it. 2) We are requesting clarification of CIP-006-1 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

Entity	Segment	Vote	Comment
			enclosed ("six wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets. The standard does not explicitly require a given ESP to be fully contained by a single PSP. We request a clarifying interpretation which allows an ESP to span multiple PSPs provided that communications within the ESP are protected sufficiently to prevent unauthorized access. Commentary: With the use of encrypted tunnels and physical protection of the tunnel endpoints, we believe that secure, CIPS compliant ESPs can be designed which span multiple PSPs. It should be noted that 005.R1.3 defines communication links between ESPs as an "access point", which in turn requires port/protocol restrictions at the access point (005.R2.2). However, OSI layer 3 controls won't solve what is fundamentally an OSI layer 2 concern. Specifically, port and protocol restrictions at the endpoints of a frame relay connection will not adequately mitigate the risk of exposure to packets being manipulated at OSI Layer 2. Hence, our desire to use encrypted tunnels to assure packet integrity and source authenticity thereby addressing the layer 2 concerns. Thank you for the opportunity to comment.
Response: The RFI response team agrees with the comment that the main objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. In regard to wiring, the RFI response drafting team asserts that the definition of Cyber Asset in the NERC Glossary indeed includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. With respect to the commentary about a single ESP spanning multiple PSPs, the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 applies. The drafting team is not familiar with the October 10, 2007 RFI by Puget Sound Energy.			
Salt River Project	1	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat.
Response:			

Entity	Segment	Vote	Comment
The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Seattle City Light	1	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.

Response:

The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.

The scenario described in this comment wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring.

The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection.

The recommendation to address data in motion is currently included in the work of the CSO706 Project.

Entity	Segment	Vote	Comment
Sierra Pacific Power Co.	1	Negative	This interpretation seems to expand the applicability of the CIP Requirements outside the bounds of the Critical Assets.
Response: The RFI response drafting team does not expand the applicability of the CIP requirements but states the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			
Southern California Edison Co.	1	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team's proposed interpretation for CIP-006-1's Requirement 1.1 ("Proposed Interpretation"). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that "Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." SCE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE's communications network, and the data which streams across it, is strictly controlled by an Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rites dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that			

Entity	Segment	Vote	Comment
is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, the request from Progress Energy must be addressed in the formal Interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Southern Company Services, Inc.	1	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The phrase "alternative measures" in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Southwest Transmission Cooperative, Inc.	1	Negative	"The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response:			

Entity	Segment	Vote	Comment
The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team believes alternative measures is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible.			
Tampa Electric Co.	1	Negative	Tampa Electric Company’s Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry’s attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security “ such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.

Entity	Segment	Vote	Comment
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Tennessee Valley Authority	1	Negative	While we agree that physical and electronic perimeters must be the same or the data must protected as it traverses physical perimeters, TVA doesn't think that the interpretation provides sufficient detail to guide compliance.
Response: The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team is limited in its ability to provide more explicit guidance and believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tucson Electric Power Co.	1	Negative	TEP supports the following provided by WECC: "The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to			

Entity	Segment	Vote	Comment
avoid such language.			
Westar Energy	1	Negative	Disagree with the concept that wire is a Cyber Asset.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			
Western Area Power Administration	1	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to "wires within a given facility or campus" and therefore doing so is unjustified. The drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Xcel Energy, Inc.	1	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on

Entity	Segment	Vote	Comment
			entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope. The team understands the desire for more specificity and prescription such as in a diagram but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
British Columbia Transmission Corporation	2	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
California ISO	2	Negative	The interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with “what should have been done”. The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address. Conflicts: the interpretation crosses multiple standards CIP-006-1, 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-005-1, R1.3: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)."

Entity	Segment	Vote	Comment
			Glossary: "Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data." The reference in CIP-005, R1.3 describes "communication links"; in reality, those links are the "wiring" that the interpretation request is describing; thus, they are not within the Electronic Security Perimeter and do not need to be within a Physical Security perimeter.
Response: The RFI response drafting team recognizes that while data in transit is fundamentally the asset to be protected, it agrees that the CSO706 Project is where it should be addressed. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Independent Electricity System Operator	2	Negative	Although directionally the IESO is in favour of the intent of the interpretation, we believe the current interpretation wording may effectively modify the intention of the standard, which is inconsistent with NERC standard development protocol, and hence the interpretation needs more work. CIP-006-1, R1.1 states: "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(emphasis added) to the Critical Cyber Assets." the interpretation states: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring OR ALTERNATIVE PROTECTIVE MEASURES(emphasis added). Whereas the standard clearly requires physical access control, the interpretation effectively relaxes this requirement with the words either through physical protection of the wiring or alternate protective measures where the resultant implication is that the alternate protective measures are non-physical, hence a relaxation of the standard. Although we believe the standard should be revised to allow alternative protective measures, that is not the issue being balloted.
Response: The RFI response drafting team respectfully disagrees that the scope of alternative measures does not include logical approaches. The drafting team concurs that the intent is to protect the data that travels over the wiring and asserts that either physical or logical measures are capable of achieving the desired objective.			
ISO New England, Inc.	2	Negative	There are three significant issues with this Interpretation which resulted in a negative vote: (1) the interpretation adds requirements that are not already part of the Standard, the Standard intentionally did not originally address data in transit over communication links; (2)the interpretation creates conflicts between CIP-006 R1.1 and CIP-005, R1.3, which clearly states that communication links connecting discrete ESPs shall not be considered part of the ESP; and (3) we believe that the current Standard is clear enough and this interpretation simply creates more confusion in the industry, we have not had any problems in understanding or implementing

Entity	Segment	Vote	Comment
			the Requirements in this Standard.
Response: (1) The notion of data in transit, while at the core of the protection purpose, is more appropriately addressed in the ongoing CSO706 Project. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. (2) Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP. (3) The drafting team is compelled by process to respond to this RFI from Progress Energy.			
Midwest ISO, Inc.	2	Negative	The FAQ developed along with the original CIP standards specifically state that the standards are not intended to address the wires between facilities. While we agree that the suggested interpretation is a good idea for a future improvement to the standard, the interpretation process is intended to clarify what the standard says as originally drafted, not what we would like the standard to say.
Response: The FAQ is a guidance document and is not mandatory and enforceable as NERC standards are. However, question #11 (reproduced below) refers to assets that are not owned by the Responsible Entity, such as third party telecommunications company equipment. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. In this instance, the wiring referenced by Progress Energy is clearly within a single ESP. **11. FAQ - Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?* **Answer:** Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset.			
PJM Interconnection, L.L.C.	2	Negative	PJM has the following concerns: Procedural: the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address. Conflicts: the interpretation crosses multiple standards CIP-006-1, 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-005-1, R1.3: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)." Glossary: "Cyber Assets: Programmable

Entity	Segment	Vote	Comment
			electronic devices and communication networks including hardware, software, and data." The reference in CIP-005, R1.3 describes "communication links"; in reality, those links are the "wiring" that the interpretation request is describing; thus, they are not within the Electronic Security Perimeter and do not need to be within a Physical Security perimeter. Necessity: the definitions and descriptions contained within the published standard seem clear; the issue has posed no significant problems for SWG member organizations to understand or implement.
Response: The RFI response drafting team recognizes that while data in transit is fundamentally the asset to be protected, it agrees that the CSO706 Project is where it should be addressed. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Alabama Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
American Electric Power	3	Negative	Although we agree that a true "systems" approach to data protection would also include the data paths, we are concerned about an element that we believe should be included in any determination of communication path physical security. Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively

Entity	Segment	Vote	Comment
			accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Consolidated Edison Co. of New York	3	Negative	The interpretation is not clear, may modify the intention of the Standard, and needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Consumers Energy	3	Negative	Consumers Energy’s understanding of the requirements of CIPS-005-1 and CIPS-006-1 as they were being developed and as they exist today allowed for discrete non-contiguous physical security perimeters to protect cyber assets contained within a single electronic security perimeter, presumably by excluding the communication network and data passing over the communication network as being defined as Cyber Assets requiring physical protection. We believe that this view is consistent with good utility practice utilized at a number of North America’s control centers and generating plants. In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the original drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems or devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, and none of the nine requirements specifically address network cables or data. Had the original intent of the standards been to include the communication networks within an electronic security perimeter as Cyber Assets requiring physical protection we would have expected the standard to address appropriate protection where six-wall physical protection (complete with access control

Entity	Segment	Vote	Comment
			and monitoring) is not necessary (such as with buried portions of the network) or practical (such as within raceways or conduit). Additionally, the time required to re-wire such networks so as to provide six-wall physical protection is significantly longer than the time required to provide six-wall physical protection to the access points to Cyber Assets within the Electronic Security Perimeter. Further, had the original intent of the standards been to include data that passes over the communication network, the standard should have discussed the issues associated with transporting, storing and restoring back-up tapes and other removable media so as to protect cyber assets in the event the back-up data is re-introduced to the electronic security perimeter. We suggest the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. We believe the primary intent of the present version of the CIP Standards is to protect against remote compromise of those assets. The apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards as they were developed and implemented. CIP-006-1 R1.1 states "ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter." This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting communication network cabling residing in an area entirely within the reasonable and prudent control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all communication network and data as Cyber Assets requiring physical protection, the wording should have stated such. If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between "in-house" cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. We propose the following wording to replace the existing interpretation: Response: The Physical Security Perimeter is required to protect the access points to Critical Cyber Assets within the Electronic Security Perimeter. For dedicated communication networks within a discrete Electronic Security Perimeter under the normal reasonable and prudent control of the Responsible Entity, all elements of such network do not require to be contained within the Physical Security Perimeter so long as all access points to the Critical Cyber Assets within the Electronic Security Perimeter are also within a Physical Security Perimeter. CIP-005-1 R1.1 refers to any externally connected communication end point (for example, dial-up modems) as specifically identified as an access point to the Electronic Security Perimeter. The use of "externally connected" in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be "external" would include local area networks between floors in a building or between buildings in a campus environment.
Response: The RFI response drafting team believes the commenter's presumption that protection is not required for wiring between "discrete non-contiguous physical security perimeters" is not justified. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a			

Entity	Segment	Vote	Comment
single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP. The drafting team believes that the other concerns raised by the commenter, including transfer of backup tapes and other removable media, is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project.			
Cowlitz County PUD	3	Negative	Cowlitz County PUD No.1 (District) finds the interpretation does not clarify the intent of the Standard. Extension of the "6-wall" physical security perimeter with conduit would require an accounting for all access points (condulets or conduit bodies) and appropriate access monitoring. Simple use of conduit does not offer the best protection of data as it can be easily compromised. The verbiage "or alternative protective measures" needs clarification - or alternative physical and/or logical protective measures - to protect the original intent of the Standard. The District's position is that logical protective measures (such as loss of continuity alarms) will in many cases better protect data from malicious tampering than physical protective measures.
Response: The RFI response drafting team clarifies CIP-006 R1.1 which states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Duke Energy Carolina	3	Negative	Thank you for the opportunity to vote on this interpretation. We think that the interpretation is unclear. A new NERC Cyber Security drafting team is in the process of being assembled, and Duke Energy believes that this issue is best addressed in a comprehensive manner by the new Cyber Security drafting team. The manner of protecting data from tampering when it is transmitted over networks should be clearly defined in the new Cyber Security Standard, and any newly prescribed protection methods must be properly related to other requirements in the standards where that is appropriate.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			

Entity	Segment	Vote	Comment
FirstEnergy Solutions	3	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that ""Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Georgia Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. -

Entity	Segment	Vote	Comment
			The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Gulf Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Hydro One Networks, Inc.	3	Negative	Hydro One Networks Inc. is casting a Negative vote with the following comment: The interpretation is not clear and may modify the intention of the Standard. It needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter," which must be protected. While the wires connecting two ESPs need to be protected it should not make one PSP of both. Appropriate conduit or similar protection as appropriate should be acceptable.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the			

Entity	Segment	Vote	Comment
connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. Appropriate conduit, as suggested by the commenter, is an acceptable physical protection.			
Lincoln Electric System	3	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 applies.			
Madison Gas and Electric Co.	3	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the

Entity	Segment	Vote	Comment
			explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal Interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team disagrees with the commenter that the exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Manitoba Hydro	3	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			

Entity	Segment	Vote	Comment
However, the drafting team disagrees with removal of the term communication network in the RFI response as it already referenced in the NERC Glossary.			
MidAmerican Energy Co.	3	Negative	MidAmerican Energy believes that this interpretation expands the requirements of the standard inappropriately.
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Mississippi Power	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-1 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
New York Power Authority	3	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "... all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimieter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a			

Entity	Segment	Vote	Comment
completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Niagara Mohawk (National Grid Company)	3	Negative	The interpretation is not clear and may modify the intention of the Standard and therefore needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimieter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Platte River Power Authority	3	Negative	The interpretation would be acceptable if language is added similar to what is suggested below: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering. Where (“six-wall”) physical protection of the wiring cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to			

Entity	Segment	Vote	Comment
physical tampering.			
Public Utility District No. 2 of Grant County	3	Affirmative	
Salt River Project	3	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat.
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Seattle City Light	3	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.
Response: The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			

Entity	Segment	Vote	Comment
The scenario described by the commenter wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection. The recommendation to address data in motion is currently included in the work of the CSO706 Project.			
Tampa Electric Co.	3	Negative	Tampa Electric Company’s Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry’s attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: • These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. • The primary DCS vendors in our environment do not offer or support an approved mechanism for encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. • The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective

Entity	Segment	Vote	Comment
			based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: • Unauthorized access to the ESP through access to physical cabling. • Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. • Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.			
Wisconsin Public Service Corp.	3	Negative	The interpretation for CIP-006 significantly expands the scope of the standard and needs to go through through the SAR process. The inclusion of communications network wiring is a shift from previous industry understanding and is contrary to responses for Frequently Asked Questions posted on the NERC website. Standard CIP-002-1 — Cyber Security — Critical Cyber Assets 11. Question: Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards? Answer: Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset. Standard CIP-005-1 Cyber Security — Electronic Security 2. Question: I am connected to other partners Electronic Security Perimeters through a Wide Area Network (WAN) connection. What is now included in the Electronic Security Perimeter? Is the connection to the partner included? Answer: The standard states that where discrete Electronic Security Perimeters are connected by communication lines, the communication lines are not included in the Electronic Security Perimeter. 15. Question: Is a physically isolated and dedicated network required for connections between Electronic Security Perimeters? Answer: No, physical isolation is not required, nor is a dedicated link required. The standard does not specify any requirement for communication between discrete Electronic Security Perimeters, since this is currently beyond the scope of these standards. It

Entity	Segment	Vote	Comment
			is possible for the data between discrete perimeters to be carried over a shared infrastructure such as a shared WAN, or to be carried over dedicated links. However, the Responsible Entity must ensure that the access control devices (such as firewalls) at the access points to the Electronic Security Perimeters do not permit unauthorized access to the Electronic Security Perimeters and the Cyber Assets within them. When data is carried over a shared infrastructure, the Responsible Entity should ensure as well that the data has not been changed in transit. Logical or virtual separation of the data in a shared infrastructure can be accomplished by using existing technologies such as virtual circuits and communication tunnels. Encryption or other data integrity checking technologies can also ensure that data is not changed in transit, provided performance and latency requirements for the applications are satisfied. Standard CIP-006-1 — Cyber Security — Physical Security 20. Question: Does the standard require entities to protect telecommunications services and facilities that serve physical security system assets? Answer: CIP-002 through CIP-009 do not address telecommunications.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. The RFI response team clarifies in a revised interpretation response that physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. Protection of communication systems that reside within an ESP is required. The Frequently Asked Questions posted on the NERC website is a guidance document and is not mandatory and enforceable as NERC standards are. However, question #11 (reproduced below) refers to assets that are not owned by the Responsible Entity such as third-party telecommunications company equipment. **11. FAQ - Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?* **Answer:** Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset. In addition, the figure associated with Question 2 for CIP-005-1 (Page 12 of the FAQ) specifically addresses the commenter's concerns regarding interconnectivity of ESP's over Wide Area Networks. This interpretation does not change the exclusion of communication networks outside of an ESP from the standard. In this instance the wiring is clearly stated by Progress Energy to be within a single ESP.			
Xcel Energy, Inc.	3	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these

Entity	Segment	Vote	Comment
			rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Alliant Energy Corp. Services, Inc.	4	Negative	CIP-005 - R1.3 specifically excludes the connecting cabling from the CIP standards. There can not be such conflicting statements between standards.
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Consumers Energy	4	Negative	Consumers Energy's understanding of the requirements of CIPS-005-1 and CIPS-006-1 as they were being developed and as they exist today allowed for discrete non-contiguous physical security perimeters to protect cyber assets contained within a single electronic security perimeter, presumably by excluding the communication network and data passing over the communication network as being defined as Cyber Assets requiring physical protection. We believe that this view is consistent with good utility practice utilized at a number of North America's control centers and generating plants. In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the original drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems or devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, and none of the nine requirements specifically address network cables or data. Had the original intent of the standards been to include the communication networks within an electronic security perimeter as Cyber Assets requiring physical protection we would have expected the standard to address appropriate protection where six-wall physical protection (complete with access control and monitoring) is not necessary (such as with buried portions of the network) or practical (such as within raceways or conduit). Additionally, the time required to re-wire such networks so as to provide six-wall physical protection is significantly longer than the time required to provide six-wall physical protection to the access points to Cyber Assets within the Electronic Security Perimeter. Further, had the original intent of the standards been to include data that passes over the communication network, the standard should have discussed the issues associated with transporting, storing and restoring back-up tapes and other removable media so as to protect cyber assets in the event the back-up data is re-introduced to the electronic security perimeter. We

Entity	Segment	Vote	Comment
			suggest the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. We believe the primary intent of the present version of the CIP Standards is to protect against remote compromise of those assets. The apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards as they were developed and implemented. CIP-006-1 R1.1 states "ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter." This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting communication network cabling residing in an area entirely within the reasonable and prudent control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all communication network and data as Cyber Assets requiring physical protection, the wording should have stated such. If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between "in-house" cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. We propose the following wording to replace the existing interpretation: Response: The Physical Security Perimeter is required to protect the access points to Critical Cyber Assets within the Electronic Security Perimeter. For dedicated communication networks within a discrete Electronic Security Perimeter under the normal reasonable and prudent control of the Responsible Entity, all elements of such network do not require to be contained within the Physical Security Perimeter so long as all access points to the Critical Cyber Assets within the Electronic Security Perimeter are also within a Physical Security Perimeter. CIP-005-1 R1.1 refers to " any externally connected communication end point (for example, dial-up modems) " as specifically identified as an access point to the Electronic Security Perimeter. The use of "externally connected" in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be "external" would include local area networks between floors in a building or between buildings in a campus environment.

Response:

The RFI response drafting team believes the commenter's presumption that protection is not required for wiring between "discrete non-contiguous physical security perimeters" is not justified. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies.

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

Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.

Entity	Segment	Vote	Comment
The drafting team believes that the other concerns raised by the commenter, including transfer of backup tapes and other removable media, is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project.			
Madison Gas and Electric Co.	4	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team disagrees with the commenter that exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-			

Entity	Segment	Vote	Comment
006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Seattle City Light	4	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.
Response: The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006. The scenario described by the commenter wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection. The recommendation to address data in motion is currently included in the work of the CSO706 Project.			

Entity	Segment	Vote	Comment
Seminole Electric Cooperative, Inc.	4	Negative	Seminole endorses the comments of Tampa Electric Company as replicated below: Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. We have several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach my be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment do not offer or support an approved mechanism for encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, we recommend that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.

Response:

The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden.

Entity	Segment	Vote	Comment
However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Wisconsin Energy Corp.	4	Negative	Interpetation is overreaching
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
WPS Resources Corp.	4	Negative	The interpretation for CIP-006 significantly expands the scope of the standard and needs to go through through the SAR process. The inclusion of communications network wiring is a shift from previous industry understanding and is contrary to responses for Frequently Asked Questions posted on the NERC website.
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
AEP Service Corp.	5	Negative	Although we agree that a true "systems" approach to data protection would also include the data paths, we are concerned about an element that we believe should be included in any determination of communication path physical security. Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or inobtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response:			

Entity	Segment	Vote	Comment
The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Allegheny Energy Supply Company, LLC	5	Negative	Allegheny Energy is concerned with the SAR drafting team interpretation that wiring within an ESP be considered a Cyber Asset or Critical Cyber Asset. Allegheny Energy agrees that the wiring (and information transmitted by such wiring) within an ESP needs to be protected; however, Allegheny Energy does not agree that the wiring needs to be classified and protected as a defined cyber asset. NERC defines cyber assets as programmable electronic devices and communication networks including hardware, software, and data and does not include the language “including the wiring that comprises the physical media supporting the network”. Allegheny Energy believes the best method to determine protection measures for the wiring (and information transmitted by such wiring) is to create a holistic approach to communication network and data communication link protection through the Standards process that specifically addresses these issues. This new Standard could address communication network and data communication link security issues, including copper cabling, fiber optic cabling, and wireless implementations. By the interpretation stating that network wiring is a cyber asset or potentially a critical cyber asset in an effort to physically secure the wiring, this statement would additionally impose all of the requirements of the CIP standard that are applicable to cyber assets and in essence make entities non-compliant since many requirements cannot be accomplished for wiring.
Response: The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. As such the RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
City of Tallahassee	5	Negative	CIP-005-1, R1.3 states: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)."

Entity	Segment	Vote	Comment
			Since it is not within the Electronic Security Perimeter, it does NOT need to be within a Physical Security perimeter that is required in CIP-006-1, R1.1. (Glossary) Cyber Assets: "Programmable electronic devices and communication networks including hardware, software, and data." I disagree that this includes the "wires". The "communication links connecting" are the "wires" and they are excluded per CIP-005, R1.3. We cannot have one standard saying the wires are included and another saying they are not!
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Colmac Clarion/Piney Creek LP	5	Affirmative	Appears to adequately require either 'six boundary' enclosure or entity description of protective measures on wiring or components outside of same. Doesn't require that entity methods equal six wall protection however.
Response: Thank you for your comment. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Consumers Energy	5	Negative	Consumers Energy’s Comments to Accompany a “No” Vote on NERC 2008-10 August 6, 2008 **2008-10 Goes Beyond the Intent of the Standards** In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems, devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, not network cables or data. **Data and Cables Would Become Critical Cyber Assets** If this interpretation passes, network cables and data will be considered Cyber Assets. Since it is difficult to conceive of an Asset that uses a network where data and networks are not essential to the operation of that Asset, data and network cabling will become Critical Cyber Assets. This will be true for control centers, generating plants and substations. **Data as a Critical Cyber Asset** The act of identifying data as a Critical Cyber Asset has far-reaching implications. Will removable media such as backup tapes need to be stored within an Electronic Security Perimeter? How can media so protected be

Entity	Segment	Vote	Comment
			moved to an off-site storage location? **Actual Intent - Cyber Asset Has CPU** Consumers Energy suggests the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. Consumers Energy further suggests the primary intent of the present version of the CIP Standards is to protect against remote compromise. **Intent of Interpretation Goes Too Far for This Stage** Consumers Energy also suggests that the apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards in their present form. CIP-006-1 R1.1 states “ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.” This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting network cabling residing in an area entirely within the control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all connections outside the ESP, the wording should have stated such. Threats and Priorities If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between “in-house” cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. **Proposed Rewording** Consumers Energy proposes the following wording to replace the existing interpretation: Response: CIP-006-1 R1.1 refers to “any externally connected communication end point (for example, dial-up modems)” as specifically identified as an access point to the Electronic Security Perimeter. The use of “externally connected” in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be ”external” would include local area networks between floors in a building or between buildings in a campus environment.

Response:

On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.

The RFI response drafting team agrees and acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also notes that Critical Cyber Asset classification is an important issue and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. Therefore, the

Entity	Segment	Vote	Comment
matter of data protection is not directly address by this RFI response. The drafting team does not agree that protection of only Cyber Assets with CPUs is the intent of the CIP standards. The drafting team believes that the requirement clearly states that “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team appreciates the suggested replacement wording, but believes it does not meet the objective of CIP-006-1.			
Detroit Edison Company	5	Negative	The following are Detroit Edison's reasons for voting No: The NERC Glossary defines Cyber Assets as “Programmable electronic devices and communication networks including hardware, software, and data”. Detroit Edison believes that this definition relating to the network is to include active devices that comprise the network, not the transmission media itself. Thus routers, switches, hubs, etc. are cyber assets, wiring is not. Detroit Edison's opinion on protecting cabling between physical security perimeters fully contained within an otherwise adequately secured facility is that the cable is sufficiently protected following guidance provided by NIST. Additional protection can be provided by covering the cable trays where they are easily accessible. "NIST SP800-53 PE-4 Access Control For Transmission Medium, Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays." Note that conduit and cable tray is specified as adequate protection by NIST however, if the interpretation is approved as written a completely enclosed six wall boundary would be required. Does this mean that all conduit bodies, pull boxes, cable tray covers, and open cable trays would become access points subject to CIP-006? "FERC Order 706 paragraph 224: Congressional Representatives state that NIST research prepared a technical report comparing the proposed CIP Reliability Standards with SP 800-53. This technical report found that an organization conforming to the baseline set of security controls in SP 800-53 will also comply with the management, operational and technical security requirements of the CIP Reliability Standards, though the converse may not be true." Detroit Edison believes that the outer barrier cable jacket, designed and manufactured to protect the data transport media within the jacket, represents a comprehensive six wall cable barrier and furthermore, completely enclosing wiring between physical security perimeters with a second protective measure such as a conduit, would be unduly burdensome, increase the risk of creating adjacency hazards and would not significantly improve the security posture of the critical cyber assets in the electronic security perimeter. Detroit Edison further supports the use of alternative protective measures such as data encryption where technically feasible, over the use of conduit,

Entity	Segment	Vote	Comment
			which significantly provides enhanced security over the use of conduit alone.
Response: On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The examples of cable protection cited in the comment appear to be viable physical approaches; however, the conclusion that a six-wall bounded physical solution is the only acceptable one is not accurate. The Requirement R1.1 of CIP-006-1 clearly states that “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
FirstEnergy Solutions	5	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that “Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter.			

Entity	Segment	Vote	Comment
The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Lincoln Electric System	5	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: Thank you for your comment. The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Manitoba Hydro	5	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the drafting team disagrees with removal of the term communication network in the RFI response, as it already referenced in the NERC Glossary.			

Entity	Segment	Vote	Comment
Northern States Power Co.	5	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Pacific Gas and Electric Company	5	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” i not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			

Entity	Segment	Vote	Comment
PPL Generation LLC	5	Negative	Response: The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.
Response: The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.			
Reliant Energy Services	5	Negative	Reliant Energy is in agreement with the following comment posted by First Energy at 3:54 pm on August 13, on PJM’ NERC Standard e-Room. That is; “he definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly; the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team agrees that protection can be provided through alternative measures that include use of a combined/complementary physical and logical approach to achieve the same or better protection.			
Salt River Project	5	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			

Entity	Segment	Vote	Comment
Southern California Edison Co.	5	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team' proposed interpretation for CIP-006-1's Requirement 1.1 (Proposed Interpretation). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." CE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE's communications network, and the data which streams across it, is strictly controlled by an Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rights dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.

Response:

The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.

However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.

The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current

Entity	Segment	Vote	Comment
Requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tampa Electric Co.	5	Negative	Tampa Electric Company's Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: • These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. • The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. • The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations. We believe

Entity	Segment	Vote	Comment
			that the Standard Authorization Request should be modified to address concerns and issues related to: • Unauthorized access to the ESP through access to physical cabling. • Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Tennessee Valley Authority	5	Negative	The factors, which lead to this conclusion, are the exponential increase in scope and cost for the implementation of physical security applied to the communication media.
Response: CIP-006-1 requires all Cyber Assets within an ESP to be enclosed within a PSP. The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden.			
U.S. Bureau of Reclamation	5	Negative	This issue raises a question as to the NERC requirements for the physical protection of critical cyber assets that fall outside of readily defined Physical Security Perimeters (PSPs). The connection between the two PSPs is a communications line employing a routable protocol and may be based on microwave, radio, copper, or fiber technologies. For circuits that go between physical structures separated by more than several feet, the 6 wall requirement is impractical. NERC's response to the question raised was consistent with their overall requirements in the sense that they did not relax protection requirements for Critical Cyber Assets (specifically wiring) external to an Electronic Security Perimeter (ESP). Reclamation will be significantly impacted by this interpretation for its Critical Cyber Systems that extend over several physical sites. Specifically in cases where those sites are interconnected with communications circuits employing "routable protocols." In those instances, since physical protection of the circuits will be impractical or impossible, Reclamation will need to employ "alternate protective measures" on communications lines interconnecting the physically distinct sites. We suggest NERC reconsider their requirements in cases where interconnections between sites remain within the same "control system" and where those interconnections are carried over privately owned circuits. The

Entity	Segment	Vote	Comment
			requirements NERC has outlined make very good sense (and we support them) where the connections go to external entities or where they are carried over public networks. We have no desire to change this aspect of the requirements. We are requesting special consideration be given to private networks between physical and electronic perimeters where those networks are owned/operated by the entities in question.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. The RFI response team is limited to interpreting the requirement of the existing standard. The request for consideration of private networks is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.			
AEP Marketing	6	Negative	Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Consolidated Edison Co. of New York	6	Negative	The interpretation is not clear and may modify the intention of the Standard and needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring			

Entity	Segment	Vote	Comment
needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
FirstEnergy Solutions	6	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple			

Entity	Segment	Vote	Comment
physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Lincoln Electric System	6	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: Thank you for your comment. The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Madison Gas and Electric Co.	6	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?

Entity	Segment	Vote	Comment
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team disagrees with the commenter that exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Manitoba Hydro	6	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the drafting team disagrees with removal of the term communication network in the RFI response, as it already referenced in the NERC Glossary.			
PP&L, Inc.	6	Negative	Response: The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The

Entity	Segment	Vote	Comment
			intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.
Response: The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.			
Salt River Project	6	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Southern California Edison Co.	6	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team’s proposed interpretation for CIP-006-1’s Requirement 1.1 (Proposed Interpretation). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that “Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network.” SCE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE’s communications network, and the data which streams across it, is strictly controlled by an

Entity	Segment	Vote	Comment
			Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rights dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current Requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tampa Electric Co.	6	Negative	Tampa Electric Company's Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level

Entity	Segment	Vote	Comment
			of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Xcel Energy, Inc.	6	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could

Entity	Segment	Vote	Comment
			still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
California Energy Commission	9	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to "wires within a given facility or campus" and therefore doing so is unjustified. The drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Commonwealth of Massachusetts Department of Public Utilities	9	Negative	The interpretation should not include speculation as to the intent of the reliability standard.
Response:			

Entity	Segment	Vote	Comment
The RFI response drafting team does not speculate but rather interprets the standard as permitting "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Oregon Public Utility Commission	9	Negative	The interpretation should not include speculation as to the intent of the standard. The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response drafting team does not speculate but rather interprets the standard as permitting "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response, and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset and would thus not qualify in and of itself as a Critical Cyber Asset. The drafting team believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Electric Reliability Council of Texas, Inc.	10	Negative	This interpretation is an issue that should be handled through the full Standard review process.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is			

Entity	Segment	Vote	Comment
among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Midwest Reliability Organization	10	Negative	MRO Response: CIP-005-1, R1.3 states: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)." Since it is not within the Electronic Security Perimeter, it does NOT need to be within a Physical Security perimeter that is required in CIP-006-1, R1.1. (Glossary) Cyber Assets: "Programmable electronic devices and communication networks including hardware, software, and data." The MRO disagrees that this includes the "wires". The "communication links connecting" are the "wires" and they are excluded per CIP-005, R1.3. We cannot have one standard saying the wires are included and another saying they are not!
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
SERC Reliability Corporation	10	Negative	The interpretation indicates that the definition of a Cyber Asset includes the wiring that comprises the physical media supporting the [communications] network -- although this is not included in the NERC Glossary definition. The interpretation goes on to state that the intent is to protect the “data” transmitted over the network within the Electronic Security Perimeter rather than to protect “the facilities, systems, and equipment which if destroyed, degraded, compromised or otherwise rendered unavailable, would affect the reliability of the Bulk Electric System as a whole, not risk to a Responsible Entity’s individual asset” as described in Security Guidelines for the Electric Sector: Identifying Critical Assets. The interpretation merely restates the requirement of CIP-006-1, R1.1 to take (either Physical Security Perimeter or alternative) measures to control physical access of Critical Cyber Assets and adds confusion to the standard by introducing concepts contrary to other reference material provided by NERC.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			

Entity	Segment	Vote	Comment
Southwest Power Pool	10	Negative	SPP believes the concerns raised in this interpretation are too important to let lie in an interpretation. Although the interpretation provides additional guidance about the intent of the standard, it is not good practice to keep the requirement as written. A rewrite of R1.1 under a clear scope is a better way for the industry to understand the intent.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Western Electricity Coordinating Council	10	Negative	“The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus.” “If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.”
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on Initial Ballot — Interpretation - CIP-006 - Cyber Security — Physical Security of Cyber Security Assets (Project 2008-10)
Date of Initial Ballot: September 30, 2009 – October 12, 2009

Summary Consideration:

The interpretation drafting team thanks all who commented during the last posting of the revised interpretation for their interest and feedback. Commenters from the last posting of the revised interpretation provided constructive comments and concerns. The interpretation drafting team identified two general themes in the comments:

1. **Disagreement concerning whether wiring is a "Cyber Asset." Several commenters expressed concern that interpreting wiring within the definition of "Cyber Asset" expanded the requirements of the standard; and**
2. **That CIP-006-1, requirement R1.1 does not specifically discuss particular options that may be used as alternatives to a completely enclosed ("six-wall" border) and should not be addressed by this interpretation.**

In response to the comments received and reflective of the team's revisions to the interpretation, the interpretation drafting team responded as follows:

The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.

The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Voter	Entity	Segment	Vote	Comment
Edward P. Cox	AEP Marketing	6	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss

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

Voter	Entity	Segment	Vote	Comment
				wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Brock Ondayko	AEP Service Corp.	5	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Jason L. Murray	Alberta Electric System Operator	2	Negative	The AESO agrees that use of encryption and other logical access control methods may be sufficient in some cases, however that is not what the standard calls for. Logical access controls cannot provide physical protection, and the standard clearly calls for physical protection. Thus, this interpretation would have the effect of changing the standard. Standards are not to be changed through an interpretation. If the standard needs to be changed, then the AESO recommends that a drafting team be assembled to propose changes to the standard requirements.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Kenneth Goldsmith	Alliant Energy Corp. Services, Inc.	4	Negative	Wiring itself does not possess programmable intelligence, is not a cyber asset, and should not require the protection as detailed in CIP-006-1, R1. This level of protection will require entities to make considerable investments into atypical cable protection methods without a correpsonding gain in protection of the cyber assets within the ESP or the reliability of the Bulk Electric System.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				

Voter	Entity	Segment	Vote	Comment
Kirit S. Shah	Ameren Services	1	Negative	Requirement R1.1 does not specifically discuss wiring. However, the interpretation results in expanding this requirement.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				
Paul B. Johnson	American Electric Power	1	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Raj Rana	American Electric Power	3	Negative	n reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Jason Shaver	American Transmission Company, LLC	1	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), ATC has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Neither Requirement R1.1 (CIP-006-1) nor Requirement 3 (CIP-002-1) specifically discuss or identify wiring as a cyber asset which would need protection within a six wall barrier.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Paul Rocha	CenterPoint Energy	1	Negative	Upon further review of the interpretation provided for CIP_006-1 - R1.1, CenterPoint Energy agrees with the concerns of American Electric Power (AEP). The first part of R1.1 requires that "all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. " Therefore, it is our conclusion that the interpretation includes reference to a condition that should not occur if the entity is to be in compliance with CIP_006-1 - R1.1. Specifically, the statement pertaining to "wiring within the Electronic Security Perimeter that is external to a Physical Security Perimeter,..." should not occur (according to the requirements of R.1.1) and adds a level of complexity to what components/assets are covered and what is expected for compliance.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				
Daniel Herring	Detroit Edison Company	4	Negative	Detroit Edison's opinion is this interpretation is unnecessary and that protecting cabling between physical security perimeters fully contained within an otherwise adequately secured facility is that the cable is sufficiently protected following guidance provided by NIST for use in our nuclear plants.
Response: The IDT thanks you for your comment. While the team believes that this comment suggests a good practice, it believes that the comment is beyond the scope of the interpretation.				
Jalal (John) Babik	Dominion Resources, Inc.	3	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by "Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				

Voter	Entity	Segment	Vote	Comment
Mike Garton	Dominion Resources, Inc.	5	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by 'Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Louis S Slade	Dominion Resources, Inc.	6	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by "Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
William L. Thompson	Dominion Virginia Power	1	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by "Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Douglas E. Hils	Duke Energy Carolina	1	Negative	Thank you for the opportunity to vote on this interpretation. We think that the interpretation is unclear and believe that this issue is best addressed in a comprehensive manner in a revision to the CIP standards.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Walter Yeager	Duke Energy Carolina	6	Negative	Thank you for the opportunity to vote on this interpretation. We think that the interpretation is unclear and believe that this issue is best addressed in a comprehensive manner in a revision to the CIP standards."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is				

Voter	Entity	Segment	Vote	Comment
relevant to the “alternative measures” question that is beyond the scope of this interpretation. The definition of “Cyber Asset” in the *NERC Glossary of Terms Used in Reliability Standards* includes “communication networks,” but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of “Cyber Asset,” Requirement R1 of CIP-006-1 does not apply to wiring.				
Edward C Stein	Edward C Stein	8	Negative	So you have a system where you can detect when someone has gained "unauthorized access" and you discover that someone has gained unauthorized access, does this mean that you have violated some Standard somewhere. In today's world where the use of the internet is required to exchange market and transmission data to RTOs, I believe that it is impossible to protect yourself from a hacker. The interpretation is politically correct but is does not prevent hacking.
Response: The drafting team thanks you for your comment. While the team appreciates your concern, it believes that this issue is beyond the scope of the interpretation.				
Kent Saathoff	Electric Reliability Council of Texas, Inc.	10	Affirmative	For clarity, we suggest that NERC add a comment in guidelines or FAQs to reflect that steel conduits are acceptable as a 6-wall enclosure for wiring.
Response: The drafting team thanks you for your comment. While the team appreciates your concern, it believes that this issue is beyond the scope of the interpretation.				
John J. Blazekovich	Exelon Energy	1	Negative	Exelon believes that this interpretation, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the “alternative measures” question that is beyond the scope of this interpretation.				
Kim Warren	Independent Electricity System Operator	2	Negative	We reiterate our previous comment that although directionally the IESO is in favour of the intent of the interpretation, we believe the current interpretation wording may effectively modify the intention of the standard, which is inconsistent with NERC Reliability Standards Development Procedure. Whereas the standard clearly requires physical access control, the interpretation effectively relaxes and hence alters this requirement by permitting logical measures to control physical access. Although we believe the standard should be revised to allow alternative protective

Voter	Entity	Segment	Vote	Comment
				measures, that is not the issue being balloted. We believe revisions to CIP-006-1, Requirement R1.1 should be made in the future to specifically cater for logical measures to control physical access to the Critical Cyber Assets.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Elizabeth Howell	ITC Transmission	1	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), ITC has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Neither Requirement R1.1 (CIP-006-1) nor Requirement 3 (CIP-002-1) specifically discuss or identify wiring as a cyber asset which would need protection within a six wall barrier.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Jason L Marshall	Midwest ISO, Inc.	2	Negative	The FAQ developed along with the original CIP standards specifically state that the standards are not intended to address the wires between facilities. While we agree that the suggested interpretation is a good idea for a future improvement to the standard, the interpretation process is intended to clarify what the standard says as originally drafted, not what we would like the standard to say. In the response to comments from the initial ballot, the drafting team pointed out that the FAQ is a reference document and not enforceable. While we agree this is true, it does point out what the intent of the drafting team was when writing the requirements and is thus critical to interpreting the CIP standards. Q11 in the FAQ is clear that the drafting team did not intend to include wiring. The drafting team stated that the requirement only applies to assets that are not owned by the Responsible Entity and that the Q11 in the FAQ only addressed non-owned assets. First, we assume that the drafting team is referring to leasing by thae statement "assets that are not owned" even though leasing is one form of ownership. Second, leasing of communications cirucits is only one example given in the answer to Q11 in the FAQ. Thus, we can't conclude that Q11 does not apply to all communication circuits. If

Voter	Entity	Segment	Vote	Comment
				the drafting team wants to apply the standard to the wiring in the request for interpretation, they need to submit a SAR to modify the standard.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				
James D. Hebson	PSEG Energy Resources & Trade LLC	6	Negative	Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions on the subject. While the RFI response drating team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSEG agrees with CAL ISO's position that this interpretation should not be "....what should have been done," Southern Company's position the "....it actually reresents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice....," ISO New England's position that "....the interpretation adds requirements that are not already part of the Standard...." and PJM's position that: "....the interpretation adds requirements that are not already part of the Standard. EIP-006 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done." The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communication links between discrete perimeters, the interpretation moves into an area which the standard intentionally does no address." PSEG believes that the only appropriate was to reach agreement on Progress Energy's question is to submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum,an appropriate implementation schedule must also be issued."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Thomas Piascik	PSEG Power LLC	5	Negative	Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions for the subject. While the RFI response drafting team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSEG agrees with CAL ISO's position that this interpretation should not be "...what should have been done.", Southern Company's

Voter	Entity	Segment	Vote	Comment
				position that "...it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice...", ISO New England's position that "...the interpretation adds requirements that are not already part of the Standard..." and PJM's position that: "...the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address." PSEG believes that the only appropriate way to have agreement of Progress Energy's question is submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum, an appropriate implementation schedule must also be issued
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Kenneth D. Brown	Public Service Electric and Gas Co.	1	Negative	Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions for the subject. While the RFI response drafting team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSE&G agrees with CAL ISO's position that this interpretation should not be "...what should have been done.", Southern Company's position that "...it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice...", ISO New England's position that "...the interpretation adds requirements that are not already part of the Standard..." and PJM's position that "...the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address." PSE&G

Voter	Entity	Segment	Vote	Comment
				believes that the only appropriate way to have agreement of Progress Energy's question is submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum, an appropriate implementation schedule must also be issued.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Jeffrey Mueller	Public Service Electric and Gas Co.	3	Negative	"Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions for the subject. While the RFI response drafting team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSEG agrees with CAL ISO's position that this interpretation should not be "...what should have been done.", Southern Company's position that "...it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice...", ISO New England's position that "...the interpretation adds requirements that are not already part of the Standard..." and PJM's position that: "...the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address." PSEG believes that the only appropriate way to have agreement of Progress Energy's question is submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum, an appropriate implementation schedule must also be issued."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not				

Voter	Entity	Segment	Vote	Comment
explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Kyle M. Hussey	Public Utility District No. 2 of Grant County	1	Affirmative	I agree with this interpretation. This clarifies that wiring can not only be secured through physical means but also logical.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, approved appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Henry Delk, Jr.	SCE&G	1	Negative	SCE&G does not think the interpetation adds enough clarity. The issue should be addressed during development of the next set of NERC CIP Standards.
Response: Thank you for the comment. The Interpretation Drafting Team has revised the interpretation so that it limits itself to the specific question about wiring, and other issues raised regarding CIP-006-1 will be addressed in future versions.				
Hubert C. Young	South Carolina Electric & Gas Co.	3	Negative	SCE&G does not think the interpretation adds enough clarity. The issue should be addressed during development of the next set of NERC CIP standards.
Response: Thank you for the comment. The Interpretation Drafting Team has revised the interpretation so that it limits itself to the specific question about wiring, and other issues raised regarding CIP-006-1 will be addressed in future versions.				
Martin Bauer	U.S. Bureau of Reclamation	5	Affirmative	While Reclamation agrees with the interpretation, it is contingent on the basis that no TFE is required when Alternative Measures are deployed.
Response: Thank you for the comment. The Interpretation Drafting Team has revised the interpretation so that consideration of alternative measures and whether a TFE is required are beyond the scope of this Request for Interpretation.				
Allen Klassen	Westar Energy	1	Negative	Do not agree with wire as a cyber asset
Response: Thank you for your comment. The drafting team agrees and has revised the interpretation.				

Voter	Entity	Segment	Vote	Comment
Linda Horn	Wisconsin Electric Power Co.	5	Negative	Wisconsin Electric is concerned with the use of the term "effective security". This does not identify what type of physical protection is equivalent to six wall borders. Does cabling protected by metallic conduit constitute effective security? Communication networks utilizing fiber optic cabling is very difficult to splice in a tap allowing unapproved logical access. Does fiber optic cable require the same protective measures as copper? There are still questions or clarification required.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
James R. Keller	Wisconsin Electric Power Marketing	3	Negative	Wisconsin Electric is concerned with the use of the term "effective security". This does not identify what type of physical protection is equivalent to six wall borders. Does cabling protected by metallic conduit constitute effective security? Communication networks utilizing fiber optic cabling is very difficult to splice in a tap allowing unapproved logical access. Does fiber optic cable require the same protective measures as copper? There are still questions or clarification required.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Interpretation of CIP-006-x for Progress Energy (Project 2008-10)

The CIP-006-x for Progress Energy Drafting Team thanks all commenters who submitted comments on the interpretation for CIP-006-x for Progress Energy (Project 2008-10). These standards were posted for a 45-day public comment period from October 12, 2011 through November 21, 2011. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 17 sets of comments, including comments from approximately 56 different people from approximately 31 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2008-10_CIP-006_Interpretation_Progress.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Perry		SPP	10
2.	Shon Austin		SPP	10
3.	Ron Ciesiel		SPP	10

2.	Group	Connie Lowe	Electric Market Policy, Information Technology Risk Management	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		RFC	1
2.	Sean Iseminger		SERC	5
3.	Mike Garton		NPCC	5
4.	Michael Gildea		MRO	5

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
5. Louis Slade		RFC 6										
6. Michael Crowley		SERC 3										
3. Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Brian Evans-Mongeon	Utility Services	NPCC	8
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Chantel Haswell	FPL Group, Inc.		5
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1
11.	Michael R. Lombardi	Northeast Utilities	NPCC	1
12.	Randy Macdonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1
16.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
18.	Saurabh Saksena	National Grid	NPCC	1
19.	Michael Schiavone	National Grid	NPCC	1
20.	Wayne Sipperly	New York Power Authority	NPCC	5
21.	Tina Teng	Independent Electricity System Operator	NPCC	2
22.	Donald Weaver	New Brunswick System Operator	NPCC	2
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1
24.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3

4. Group	Nick Wehner	ACES Power Marketing Standards Collaborators						X				

Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. James Jones		Arizona Electric Power Cooperative/Southwest Transmission Company	WECC 1, 4, 5										
5.	Group	Steve Diebold	Kansas City Power & Light	X		X		X	X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Michael Gammon	KCPL	SPP	1, 3, 5, 6									
2.	Scott Harris	KCPL	SPP	1, 3, 5, 6									
3.	Dean Larson	KCPL	SPP	1, 3, 5, 6									
4.	Bob Beachy	KCPL	SPP	1, 3, 5, 6									
5.	Brett Holland	KCPL	SPP	1, 3, 5, 6									
6.	Individual	Antonio Grayson	Southern Company	X		X		X	X				
7.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
8.	Individual	Michael Falvo	Independent Electricity System Operator		X								
9.	Individual	Michael R. Lombardi	Northeast Utilities	X		X		X					
10.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
11.	Individual	Thad Ness	American Electric Power	X		X		X	X				
12.	Individual	Anthony Jablonski	ReliabilityFirst										X
13.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									
14.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
15.	Individual	Chris Higgins / Forrest Krigbaum & BPA CIP Team	Bonneville Power Administration	X		X		X	X				
16.	Individual	Rebecca Moore Darrah	MISO		X								
17.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				

1. **The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement?**

Summary Consideration:

Many commenters noted the request for interpretation is asking for clarity on the application of a requirement, while others noted the request for interpretation is asking for clarity on the meaning of a requirement. In general, the Interpretation Drafting Team ("IDT") agrees the Request for Interpretation ("RFI") asks in part for clarity on the application of the requirement ("*Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP*"). The IDT notes, however, that whether the requirement applies requires clarity on the meaning of the requirement ("*It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary*"). The IDT interpreted that "wire" is not part of the definition of "Cyber Asset," and that CIP-006-3c, R1.1, only applies to Cyber Assets, which provides clarity on the meaning and the application of the requirement.

Organization	Yes or No	Question 1 Comment
Kansas City Power & Light	The request is asking for clarity on the application of a requirement.	In this instance the request is asking for clarity in the application of the requirement, however, the interpretation response involved both the meaning of requirement CIP-002-1, R3 and the application of that meaning with CIP-006-1, R1.1.
Response: Thank you for your response. The IDT agrees the RFI appears to ask, in part, for clarity on the application of the requirement to a particular circumstance; however, the RFI also asks for clarity on the meaning of the requirement.		
ReliabilityFirst	The request is asking for clarity on the application	The last sentence of the Request for Interpretation reads (emphasis added): Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP. The meaning of the requirement appears to be reasonably clear. Progress

Organization	Yes or No	Question 1 Comment
	of a requirement.	Energy is requesting a determination of how to apply the requirement to a specific situation.
Response: Thank you for your response; the IDT agrees. The IDT agrees the RFI appears to ask, in part, for clarity on the application of the requirement to a particular circumstance; however, the RFI also asks for clarity on the meaning of the requirement.		
Southern Company	The request is asking for clarity on the application of a requirement.	The request specifically asks about the applicability of wiring.
Response: Thank you for your response; the IDT agrees. The IDT agrees the RFI appears to ask, in part, for clarity on the application of the requirement to a particular circumstance; however, the RFI also asks for clarity on the meaning of the requirement.		
Xcel Energy	The request is asking for clarity on the meaning of a requirement.	This request is defining what is considered a Critical Asset and not how to protect the Critical Assets.
Response: Thank you for the comment. The IDT agrees the interpretation provides clarity on the meaning of the requirement by clarifying that wire is not a Cyber Asset.		
Independent Electricity System Operator	The request is asking for clarity on the application	

Organization	Yes or No	Question 1 Comment
	of a requirement.	
Oncor Electric Delivery Company LLC	The request is asking for clarity on the application of a requirement.	
Southwest Power Pool Regional Entity	The request is asking for clarity on the meaning of a requirement.	
Electric Market Policy, Information Technology Risk Management	The request is asking for clarity on the meaning of a requirement.	
Northeast Power Coordinating Council	The request is asking for clarity on the meaning of a requirement.	
ACES Power Marketing Standards Collaborators	The request is asking for clarity on the	

Organization	Yes or No	Question 1 Comment
	meaning of a requirement.	
Manitoba Hydro	The request is asking for clarity on the meaning of a requirement.	
Northeast Utilities	The request is asking for clarity on the meaning of a requirement.	
Duke Energy	The request is asking for clarity on the meaning of a requirement.	
American Electric Power	The request is asking for clarity on the meaning of a requirement.	
American Transsmission Company, LLC	The request is asking for clarity on the meaning of a	

Organization	Yes or No	Question 1 Comment
	requirement.	
Bonneville Power Administration		
MISO		

2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it 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. Do you believe this interpretation expands the reach of the standard?

Summary Consideration:

Most balloters agree the interpretation does not expand the reach of the standard. However, one commenter expressed concern that the interpretation restricts the reach of the standard. In general, the IDT does not share this view, and notes that it must follow the guidelines set forth in the Guidelines for Interpretation Drafting Teams (available at: http://www.nerc.com/files/Guidelines_for_Interpretation_Drafting_Teams_Approved_April_2011.pdf). The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard.

Organization	Yes or No	Question 2 Comment
ReliabilityFirst	The interpretation does not expand the reach of the standard.	However, this interpretation greatly restricts the reach of CIP-006-3c R1.
Response: Thank you for your comment. While the IDT appreciates this concern, it disagrees that the interpretation restricts the reach of the standard. Rather, the purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard.		
Xcel Energy	The interpretation does not expand the reach of the standard.	The interpretation provided defines more clearly what should be included in the scope of standard.

Organization	Yes or No	Question 2 Comment
Response: Thank you for the comment, The IDT appreciates that its analysis of the language provides clarity.		
Southwest Power Pool Regional Entity	The interpretation does not expand the reach of the standard.	
Electric Market Policy, Information Technology Risk Management	The interpretation does not expand the reach of the standard.	
Northeast Power Coordinating Council	The interpretation does not expand the reach of the standard.	
ACES Power Marketing Standards Collaborators	The interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 2 Comment
Kansas City Power & Light	The interpretation does not expand the reach of the standard.	
Southern Company	The interpretation does not expand the reach of the standard.	
Manitoba Hydro	The interpretation does not expand the reach of the standard.	
Independent Electricity System Operator	The interpretation does not expand the reach of the standard.	
Northeast Utilities	The interpretation	

Organization	Yes or No	Question 2 Comment
	does not expand the reach of the standard.	
Duke Energy	The interpretation does not expand the reach of the standard.	
American Electric Power	The interpretation does not expand the reach of the standard.	
Oncor Electric Delivery Company LLC	The interpretation does not expand the reach of the standard.	
American Transmission Company, LLC	The interpretation does not expand the reach of the	

Organization	Yes or No	Question 2 Comment
	standard.	
MISO	The interpretation does not expand the reach of the standard.	
Bonneville Power Administration		

3. Do you agree with this interpretation? If not, why not.

Summary Consideration:

By overwhelming majority, most balloters agreed with the IDT's interpretation. However, there were some important minority viewpoints that the team considered. Almost universally, the viewpoints and concerns raised by commenters who did not agree with the interpretation were previously evaluated and considered in some manner during the development of the interpretation. In the responses that follow, and summarized here, the IDT explains the team's conclusions in developing the interpretation and how the team considered the comments. The team appreciated all of the comments and thanks participants for their input.

First, some commenters expressed concern that this interpretation conflicts with the interpretation in Appendix 1 of CIP-006-3c (see clarifying discussion, below, regarding usage of "Appendix 1" v. "Appendix 3" in reference to the interpretation developed by Project 2009-13). The IDT disagrees that this interpretation conflicts with Appendix 1, because there may be other scenarios beyond wiring for which Appendix 1 applies. Appendix 1 and this interpretation address different questions. This interpretation addresses whether wire is a Cyber Asset and Appendix 1 addresses alternative measures to a "six-wall" border for Cyber Assets.

Another commenter was concerned the interpretation would change the way standards are read and weaken the standard, but the IDT notes in its response the distinction between lists separated by "but not limited to" and the definition of "Cyber Asset," which is the subject of this interpretation. Furthermore, the IDT respectfully disagrees the interpretation weakens the standard, because the purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard.

In response to a comment that wire is a transport medium necessitating classification as a Cyber Asset and that wiring is an essential component of a network, the IDT explains that it respectfully disagrees on the bases that a transport medium is not the same as a communication network (and therefore not a Cyber Asset to which the requirement applies) and that essentiality of a component is not the criteria for application of the requirement in question.

One commenter noted the interpretation incorrectly referenced Appendix 3 of CIP-006-3c, and that the correct reference should be Appendix 1. In its interpretation, the IDT referred to the interpretation developed by Project 2009-13. That interpretation is now posted on the NERC Web site as Appendix 1 of CIP-006-3c; however, the interpretation developed by Project 2009-13 was Appendix 3 in the version of CIP-006-3c that accompanied the information for this project's (Project 2008-10) formal comment and successive ballot period materials. The numbering of the appendices in CIP-006-3c changed in September, 2011 (but not the content). The IDT agrees with the commenter that the reference should be corrected to refer to the latest posted version of CIP-006-3c, which is Appendix 1. Additionally, the IDT believes that it is clear from the context of the interpretation and the comments received that any references to "Appendix 3," both by commenters and the previously-posted version of this interpretation (Project 2008-10), refer to

the interpretation developed by Project 2009-13. In response to the comment, the IDT has changed the reference in the interpretation, which does not affect the substance of the interpretation. For purposes of these responses to comments, the IDT construes references to Appendix 1 and to Appendix 3 as references to the interpretation developed by Project 2009-13. As such, it is using the corrected reference to Appendix 1 in its responses for consistency, even if the commenter references Appendix 3.

Organization	Yes or No	Question 3 Comment
ReliabilityFirst	No	1. This interpretation is in direct conflict with Appendix 3 of CIP-006-3c. If wiring is not considered part of a network, then Appendix 3 of CIP-006-3c is not needed.2. This interpretation changes the way standards are read, and will require every reliability standard to be reviewed and possibly re-written. For example, FAC-008-3 R2.4.1 gives the scope as including, but not limited to, six types of equipment. If this interpretation passes, then FAC-008-3 will be read prescriptively. Any device not specifically listed will be out of scope for the requirement.3. From a cyber security perspective, this interpretation fatally weakens the protections of CIP-006-3c and CIP-005-3a. Running network cable outside of a Physical Security Perimeter without some form of compensating measure is exposing the data from within an ESP to possible compromise and attack.

Response: Thank you for your comments. The IDT discussed and evaluated all of these concerns in its deliberations of developing the interpretation. The following explanations, which correspond with the numbering of your comments, discuss the IDT's consideration of your concerns:

1) **The IDT disagrees that this interpretation is in direct conflict with Appendix 1 of CIP-006-3c (See explanation of "Appendix 1" v. "Appendix 3" usage in the Summary Consideration to Question 3, above). There may be other scenarios beyond wiring for which Appendix 1 applies.**
2) **The IDT respectfully disagrees. In the example given of FAC-008-3, and in many other standards' requirements, the language includes the phrase, "but not limited to," which specifically precludes a prescriptive reading of the enumerated items. Furthermore, the IDT is not changing the scope of what is enumerated in determining what is a Cyber Asset; instead, it is clarifying that "wire" is not explicitly included within the meaning of "communication network," which is enumerated in the language of the definition of "Cyber Asset."**
3) **While the IDT appreciates this concern, it disagrees that the interpretation weakens the protections of CIP-006 and CIP-005**

Organization	Yes or No	Question 3 Comment
because it is not contrary to any requirement to protect data.		
Southwest Power Pool Regional Entity	No	SPP RE does not agree with this interpretation for two reasons. 1. The NERC Glossary defines a Cyber Asset as "Programmable electronic devices and communication networks including hardware, software, and data." The wire is the transport medium for the data, and data is a cyber asset. CIP-006-3 R1.1 requires data to be protected; to protect the data, the wire must also be protected. 2. Wiring can be viewed as an essential component of the hardware comprising a network, further supporting the need to protect the wiring.
Response: The IDT thanks you for your comments. The IDT considered and evaluated these concerns in its deliberations. The following explanations, which correspond with the numbering of your comments, discuss the IDT's consideration of your concerns: **1. The IDT determined that wire is an underlying component of a Cyber Asset, much like air is the transport medium in a wireless network. However, wire or air itself is not a "communication network" (and therefore not a Cyber Asset), which is not contrary to CIP-006-3c, R1.1's requirement to protect data.** **The IDT appreciates this concern, but notes that it is outside the scope of the language of the definition of "Cyber Asset," and CIP-006-3c, R1.1's application is limited to Cyber Assets. Power and facilities are also essential components, but whether they are essential is not the criteria for application of CIP-006-3c, R1.1, which is the subject of this interpretation. The purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard.**		
Kansas City Power & Light	No	The question raised by Progress Energy is not clear enough for an appropriate interpretive response. As a result, the interpretive response may be including assumptions that were not stated in the question posed by Progress Energy. At any rate, it is recommended that Progress Energy be afforded the opportunity to resubmit their question with additional information and circumstances regarding the communications mediums leaving the Physical Security Perimeter under consideration.

Organization	Yes or No	Question 3 Comment
Response: The IDT thanks you for your comment, but it disagrees that the request for interpretation is not clear enough for an interpretive response. The IDT believes it has provided clarity to the meaning of the requirement through its analysis.		
Southern Company	Yes	However, the interpretation incorrectly refers to Appendix 3 of CIP-006-3c. The language should be corrected to refer to Appendix 1 of CIP-006-3c.
Response: The IDT thanks you for this comment. In its reference to "Appendix 3," the IDT referred to the interpretation developed by Project 2009-13. That interpretation is now posted as Appendix 1 of CIP-006-3c; however, the interpretation developed by Project 2009-13 was labeled as Appendix 3 in the version of CIP-006-3c that accompanied the information for this project's (Project 2008-10) formal comment and successive ballot period materials on the Project 2008-10 project page. The numbering of the appendices in CIP-006-3c changed in September, 2011 (but not the content). The IDT agrees with the commenter that the reference should be corrected to refer to the latest posted version of CIP-006-3c, which is Appendix 1. Additionally, the IDT believes that it is clear from the context of the comments received that references to "Appendix 3," both by commenters and the previously-posted version of this interpretation (Project 2008-10), refer to the interpretation developed by Project 2009-13. In response, the IDT has changed the reference in the interpretation, which does not affect the substance of the interpretation.		
Electric Market Policy, Information Technology Risk Management	Yes	
Northeast Power Coordinating Council	Yes	
ACES Power Marketing Standards Collaborators	Yes	
Manitoba Hydro	Yes	
Independent Electricity	Yes	

Organization	Yes or No	Question 3 Comment
System Operator		
Northeast Utilities	Yes	
Duke Energy	Yes	
American Electric Power	Yes	
Oncor Electric Delivery Company LLC	Yes	
American Transsmission Company, LLC	Yes	
MISO	Yes	
Xcel Energy	Yes	
Bonneville Power Administration		

4. Are there any other comments you would like to add that haven't been covered in the previous questions, please add them here.

Summary Consideration:

Some commenters expressed concern about the distinction between Appendix 1 of CIP-006-3c and this interpretation (See explanation of "Appendix 1" v. "Appendix 3" usage in reference to Project 2009-13 in the Summary Consideration to Question 3, above). This interpretation is distinct because it only addresses whether wire is a "Cyber Asset." The IDT notes that, while Appendix 1 may have used "wire" as an example, Appendix 1 applies only upon a determination that something is a Cyber Asset. This interpretation clarifies that wiring is not a Cyber Asset.

One commenter thought the interpretation should have been an initial ballot, but the IDT notes that a successive ballot is appropriate under the current NERC Standard Processes Manual when making a substantive change to the previously-posted interpretation.

Organization	Yes or No	Question 4 Comment
Bonneville Power Administration		BPA thanks you for the opportunity to comment on Project 2008-10 Interpretation of CIP-006-1 R1 for Progress Energy. BPA has no comments or concerns at this time.
Response: Thank you for your participation		
MISO		In general, the Midwest Independent Transmission System Operator (the "MISO") supports the revised interpretation of CIP-006-1, Requirement R1.1 (the "2008-10 Interpretation") developed by the CIP Interpretation Drafting Team (the "IDT"). In particular, MISO agrees with the IDT that wiring does not meet the definition of "Cyber Asset" in the NERC Glossary of Terms Used in Reliability Standards and that Requirement R1.1 therefore does not apply to wiring. MISO is concerned, however, that there is an inconsistency between the 2008-10 Interpretation and the interpretation in CIP-006-3c, appendix 3 ("Appendix 3"). Appendix 3 states that "[f]or Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets [ ] Requirement R1.1 as not limited to measures that are 'physical in nature'" (emphasis added). This language implies that wiring is subject to Requirement R1.1. The 2008-10 Interpretation, however, states unambiguously that

Organization	Yes or No	Question 4 Comment
		wiring is not a Cyber Asset and is not subject to Requirement R1.1. The IDT is clearly aware of this inconsistency, as it included the following language in the interpretation:This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 3. The interpretation in CIP-006-3c, appendix 3c, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).This limitation of the 2008-10 Interpretation does not, however, resolve the identified inconsistency because Appendix 3 explicitly addresses wiring, which means it is not "distinct" from the 2008-10 Interpretation. Thus, while MISO supports the approval of the 2008-10 Interpretation, MISO also urges the IDT to amend Appendix 3 or otherwise clarify that Appendix 3 does not apply to wiring.
Response: Thank you for your comment. The IDT disagrees that this interpretation is in direct conflict with Appendix 1 of CIP-006-3c (See explanation of "Appendix 1" v. "Appendix 3" usage in reference to Project 2009-13 in the Summary Consideration of Question 3, above). There may be other scenarios beyond wiring for which Appendix 1 applies. The purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard. The IDT notes that, while Appendix 1 may have used "wire" as an example, Appendix 1 applies only upon a determination that something is a Cyber Asset. This interpretation clarifies that wiring is not a Cyber Asset.		
ReliabilityFirst		This ballot should not be a successive ballot, but rather an initial ballot, as the text of the interpretation has been completely changed.
Response: The IDT thanks you for your comment, but notes that a successive ballot was called for pursuant to the NERC Standards Processes Manual. While the text completely changed, it was a substantive change necessitating a successive ballot.		
Southwest Power Pool Regional Entity		We disagree with the assertion: "This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 3. The interpretation in CIP-006-3c, appendix 3, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter

Organization	Yes or No	Question 4 Comment
		(ESP)."The interpretation in CIP-006-3C, Appendix 3 is directly applicable to Interpretation of CIP-006-1 Cyber Security - Physical Security of Critical Cyber Assets for Progress Energy. The interpretation found in Appendix 3 does provide for alternative means other than physical protection for instances in which physical protection is not technically feasible. Implementation of those alternative means addresses instances in which data must traverse beyond a traditional "six-wall" boundary.
Response: The IDT thanks you for your comment. This interpretation is distinct because it only addresses whether wire is a "Cyber Asset." The IDT notes that, while Appendix 1 may have used "wire" as an example, Appendix 1 applies only upon a determination that something is a Cyber Asset. This interpretation clarifies that wiring is not a Cyber Asset. There may be other scenarios beyond wiring for which Appendix 1 applies.		
Southern Company		We would seek guidance or direction on how this interpretation applies to all versions of the approved standards. If this guidance is already available, please include a preamble providing how the interpretation will apply to all approved versions of the CIP-006 standard (i.e. CIP versions 1 through 4).
Response: The IDT thanks you for your question. An approved interpretation will be applied as equally relevant to all prior and subsequent versions of the standard to the extent the language of the relevant requirement language is the same in substance. The IDT anticipates that this interpretation, subject to industry, NERC Board of Trustees, and FERC approval, will be equally applicable to CIP-006, Versions 1 through Version 4 (The IDT notes that Version 4 remains pending as of this response, and its answer here assumes approval as filed by NERC to FERC).		
Electric Market Policy, Information Technology Risk Management		
ACES Power Marketing Standards Collaborators		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro		
Independent Electricity System Operator		
Northeast Utilities		
Duke Energy		
American Electric Power		
Oncor Electric Delivery Company LLC		
American Transsmission Company, LLC		
Xcel Energy		

END OF REPORT

Exhibit D

Complete Record of Development of the Interpretation of Requirement R1.1 of CIP-006-4

Project 2008-10
Interpretation - CIP-006 - Cyber Security — Physical Security of Cyber Security Assets

Registered Ballot Body

Related Files

Status:
A recirculation ballot of the interpretation ended on December 19, 2011. The interpretation was approved by the ballot pool with a quorum of 88.02% and weighted segment approval of 96.04%. The interpretation will be presented to the NERC Board of Trustees for adoption in February 2012 and if adopted, filed with regulators for approval.

Background:
Progress Energy asked if Electronic Security Perimeter wiring external to a Physical Security Perimeter must be protected within a six-wall boundary.

Draft	Action	Dates	Results	Consideration of Comments
Interpretation of CIP-006-x R1 for Progress Energy Draft Interpretation Clean(21) | Redline to Last Posting(22) **Supporting Materials:** CIP-006-3C(23)	Recirculation Ballot Info(24) Vote>>	12/09/11 - 12/19/11 (closed)	Summary(25) Full Record(26)	
Interpretation of CIP-006-x R1 for Progress Energy Draft Interpretation Clean(13) | Redline to Last Posting(14) **Supporting Materials:** Unofficial Comment Form(15) CIP-006-3C(16)	Successive Ballot Vote>>	11/11/11 - 11/21/11 (closed)	Summary(18) Full Record(19)	
	Formal Comment Period Info(17) Submit Comments>>	10/12/11 - 11/21/11 (closed)		Consideration of Comments(20)
	Join	10/12/11 -		

	Ballot Pool>>	11/10/11 (closed)		
Progress Energy CIP-006-1, Requirement R1.1 - Automatic Generation Control Revised Interpretation(6) Request for Interpretation(7)	Initial Ballot Info(8) | Vote>>	09/30/09 – 10/12/09 (closed)	Summary(10) Full Record(11)	Consideration of Comments(12)
	Pre-ballot Review Info(9) | Join>>	08/31/09 – 09/30/09 (closed)		
Progress Energy CIP-006-1, Requirement R1.1 - Automatic Generation Control Interpretation(1) Request for Interpretation(2)	Initial Ballot Vote>>	08/07/08 – 08/16/08 (closed)	Full Record(4)	Consideration of Comments(5)
	Pre-ballot Window Info(3) | Join>>	07/08/08 – 08/07/08 (closed)		
To download a file click on the file using your right mouse button, then save it to your computer in a directory of your choice.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1Requirement R1.1.

In CIP-006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- *R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*
- *R3.2. The Cyber Asset uses a routable protocol within a control center; or,*
- *R3.3. The Cyber Asset is dial-up accessible.*

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The following interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the Cyber Security Order 706 SAR Drafting Team on July 2, 2008:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter**.** Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Response: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures.

From: Crews, David [mailto:david.crews@pgnmail.com]
Sent: Wednesday, April 02, 2008 5:05 PM
To: Gerry Adamski
Cc: Woods, Bruce; Goff, Edwin
Subject: Request for Interpretation CIP Standard

Progress Energy requests a formal interpretation of **CIP-006-1.** R1.1.

In **CIP_006-1**, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In **CIP-005-1,** Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In **CIP-002-1,** Requirement 3 states **"**Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

> **R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> **R3.2.** The Cyber Asset uses a routable protocol within a control center; or,
>
> **R3.3.** The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool Opens for Interpretation

Now available at: http://www.nerc.com/~filez/standards/Project2008-10_CIP-006_RFI_Progress.html

Pre-ballot Window and Ballot Pool for Interpretation of CIP-006-1 Requirement R1.1 for Progress Energy

Progress Energy submitted a Request for an Interpretation of Requirement R1.1 in CIP-006-1 — Physical Security of Critical Cyber Assets. The request asked if electronic security perimeter wiring external to a physical security perimeter must be protected within a six-wall boundary.

The Interpretation clarifies that the definition of a cyber asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the electronic security perimeter and the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures.

A new ballot pool to vote on this interpretation has been formed and will remain open up until 8 a.m. (EDT) Thursday, August 7, 2008. 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-RFI_CIP-006_Progress_in@nerc.com

Standards Development Process

The *Reliability Standards Development Procedure Manual* 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 Maureen Long, Standards Process Manager, at maureen.long@nerc.net or at (813) 468-5998.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Ballot Results	
Ballot Name:	Request for Interpretation - CIP-006-1 - Progress Energy_in
Ballot Period:	8/7/2008 - 8/16/2008
Ballot Type:	Initial
Total # Votes:	194
Total Ballot Pool:	220
Quorum:	**88.18 % The Quorum has been reached**
Weighted Segment Vote:	21.52 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			#	Fraction	#	Fraction	#	
1 - Segment 1.	63	1	10	0.196	41	0.804	4	8
2 - Segment 2.	9	0.7	0	0	7	0.7	0	2
3 - Segment 3.	53	1	9	0.209	34	0.791	5	5
4 - Segment 4.	11	1	2	0.2	8	0.8	0	1
5 - Segment 5.	42	1	11	0.306	25	0.694	2	4
6 - Segment 6.	22	1	5	0.238	16	0.762	0	1
7 - Segment 7.	1	0	0	0	0	0	0	1
8 - Segment 8.	4	0.3	2	0.2	1	0.1	0	1
9 - Segment 9.	6	0.5	1	0.1	4	0.4	0	1
10 - Segment 10.	9	0.7	1	0.1	6	0.6	0	2
Totals	**220**	**7.2**	**41**	**1.549**	**142**	**5.651**	**11**	**26**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Negative	View
1	Ameren Services Company	Kirit S. Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	Avista Corp.	Scott Kinney	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Negative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	View
1	CenterPoint Energy	Paul Rocha	Negative	

1	Central Maine Power Company	Brian Conroy		
1	City Utilities of Springfield, Missouri	Jeff Knottek	Affirmative	
1	Consolidated Edison Co. of New York	Edwin Thompson	Negative	View
1	Dominion Virginia Power	William L. Thompson	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	E.ON U.S. LLC	Larry Monday	Negative	
1	East Kentucky Power Coop.	George S. Carruba		
1	Entergy Corporation	George R. Bartlett		
1	FirstEnergy Energy Delivery	Robert Martinko	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Abstain	
1	Florida Power & Light Co.	C. Martin Mennes	Negative	
1	Great River Energy	Gordon Pietsch		
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay		
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Idaho Power Company	Ronald D. Schellberg		
1	Kansas City Power & Light Co.	Jim Useldinger	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Negative	View
1	Minnesota Power, Inc.	Carol Gerou	Affirmative	
1	Municipal Electric Authority of Georgia	Jerry J Tang	Abstain	
1	National Grid	Michael J Ranalli	Negative	View
1	Nebraska Public Power District	Richard L. Koch	Affirmative	
1	New Brunswick Power Transmission Corporation	Wayne N. Snowdon	Negative	View
1	New York Power Authority	Ralph Rufrano	Negative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Negative	
1	Northeast Utilities	David H. Boguslawski	Negative	
1	Northern Indiana Public Service Co.	Joseph Dobes	Negative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	View
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Lawrence R. Larson	Negative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Negative	View
1	PacifiCorp	Robert Williams	Negative	View
1	Potomac Electric Power Co.	Richard J. Kafka	Negative	View
1	PP&L, Inc.	Ray Mammarella	Negative	View
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Puget Sound Energy, Inc.	Catherine Koch	Negative	View
1	Sacramento Municipal Utility District	Dilip Mahendra		
1	Salt River Project	Robert Kondziolka	Negative	View
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SaskPower	Wayne Guttormson		
1	Seattle City Light	Christopher M. Turner	Negative	View

1	Sierra Pacific Power Co.	Richard Salgo	Negative	View
1	Southern California Edison Co.	Dana Cabbell	Negative	View
1	Southern Company Services, Inc.	Horace Stephen Williamson	Negative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Negative	View
1	Tampa Electric Co.	Thomas J. Szelistowski	Negative	View
1	Tennessee Valley Authority	Larry Akens	Negative	
1	Tucson Electric Power Co.	Ronald P. Belval	Negative	View
1	Westar Energy	Allen Klassen	Negative	View
1	Western Area Power Administration	Robert Temple	Negative	View
1	Xcel Energy, Inc.	Gregory L. Pieper	Negative	View
2	British Columbia Transmission Corporation	Phil Park	Negative	View
2	California ISO	David Hawkins	Negative	View
2	Electric Reliability Council of Texas, Inc.	Roy D. McCoy	Negative	
2	Independent Electricity System Operator	Kim Warren	Negative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Terry Bilke	Negative	View
2	New Brunswick System Operator	Alden Briggs		
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
3	Alabama Power Company	Robin Hurst	Negative	View
3	Allegheny Power	Bob Reeping		
3	Ameren Services Company	Mark Peters		
3	American Electric Power	Raj Rana	Negative	View
3	Atlantic City Electric Company	James V. Petrella	Negative	
3	Avista Corp.	Robert Lafferty		
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Cheney	Joe Noland	Abstain	
3	City Public Service of San Antonio	Edwin Les Barrow	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Consumers Energy	David A. Lapinski	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	Delmarva Power & Light Co.	Michael R. Mayer	Negative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	Farmington Electric Utility System	Alan Glazner		
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Negative	View
3	Florida Municipal Power Agency	Michael Alexander		
3	Florida Power & Light Co.	W.R. Schoneck	Abstain	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Negative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	

3	Great River Energy	Sam Kokkinen	Negative	
3	Gulf Power Company	Gwen S Frazier	Negative	View
3	Hydro One Networks, Inc.	Michael D. Penstone	Negative	View
3	Kissimmee Utility Authority	Gregory David Woessner	Negative	
3	Lincoln Electric System	Bruce Merrill	Affirmative	View
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	
3	Madison Gas and Electric Co.	Darl Shimko	Negative	View
3	Manitoba Hydro	Ronald Dacombe	Negative	View
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Don Horsley	Negative	View
3	New York Power Authority	Christopher Lawrence de Graffenried	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	View
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Orlando Utilities Commission	Ballard Keith Mutters	Abstain	
3	Platte River Power Authority	Terry L Baker	Negative	View
3	Potomac Electric Power Co.	Robert Reuter	Negative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Utility District No. 1 of Chelan County	Kenneth R. Johnson	Negative	
3	Public Utility District No. 1 of Pend Oreille County	Sandy Hunt	Abstain	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	View
3	Salt River Project	John T. Underhill	Negative	View
3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Tampa Electric Co.	Ronald L. Donahey	Negative	View
3	Tennessee Valley Authority	Cynthia Herron	Negative	
3	Turlock Irrigation District	Casey Hashimoto	Negative	
3	Wisconsin Electric Power Marketing	James R. Keller	Negative	
3	Wisconsin Public Service Corp.	James Maenner	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Negative	View
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Florida Municipal Power Agency	Ralph Anderson		
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Negative	View
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Negative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPS Resources Corp.	Christopher Plante	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	Allegheny Energy Supply Company, LLC	Robert Loy	Negative	View

5	Avista Corp.	Edward F. Groce	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Buckeye Power, Inc.	Kevin Koloini	Abstain	
5	City of Farmington	Clinton J Jacobs	Affirmative	
5	City of Tallahassee	Alan Gale	Negative	View
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	View
5	Conectiv Energy Supply, Inc.	Richard K. Douglass	Negative	
5	Constellation Generation Group	Michael F. Gildea	Affirmative	
5	Consumers Energy	James B Lewis	Negative	View
5	Detroit Edison Company	Ronald W. Bauer	Negative	View
5	Dynegy	Greg Mason		
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	Douglas Keegan		
5	Florida Power & Light Co.	Robert A. Birch		
5	Great River Energy	Cynthia E Sulzer	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	View
5	Louisville Gas and Electric Co.	Charlie Martin	Negative	
5	Madison Gas and Electric Co.	Steven Schultz		
5	Manitoba Hydro	Mark Aikens	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	
5	Northern States Power Co.	Liam Noailles	Negative	View
5	Orlando Utilities Commission	Richard Kinas	Negative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PPL Generation LLC	Mark A. Heimbach	Negative	View
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	Reliant Energy Services	Thomas J. Bradish	Negative	View
5	Salt River Project	Glen Reeves	Negative	View
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Southeastern Power Administration	Douglas Spencer	Affirmative	
5	Southern California Edison Co.	David Schiada	Negative	View
5	Southern Company Services, Inc.	Roger D. Green	Affirmative	
5	Tampa Electric Co.	Frank L Busot	Negative	View
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	Frank D Cuzzort	Negative	View
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	Wisconsin Public Service Corp.	Leonard Rentmeester	Negative	
6	AEP Marketing	Edward P. Cox	Negative	View
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Dominion Resources, Inc.	Louis S Slade	Negative	
6	Entergy Services, Inc.	William Franklin	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Negative	View
6	Florida Municipal Power Agency	Robert C. Williams		

6	Great River Energy	Donna Stephenson	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	View
6	Louisville Gas and Electric Co.	Daryn Barker	Negative	
6	Madison Gas and Electric Co.	Jeffrey M Keebler	Negative	View
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	PP&L, Inc.	Thomas Hyzinski	Negative	View
6	Progress Energy Carolinas	James Eckelkamp	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Negative	
6	Salt River Project	Mike Hummel	Negative	View
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Southern California Edison Co.	Marcus V Lotto	Negative	View
6	Tampa Electric Co.	Jose Benjamin Quintas	Negative	View
6	Tennessee Valley Authority	Katherine E. York	Negative	
6	Xcel Energy, Inc.	David F. Lemmons	Negative	View
7	Eastman Chemical Company	Lloyd Webb		
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	
8	Other	Michehl R. Gent		
8	Volkmann Consulting	Terry Volkmann	Affirmative	
9	California Energy Commission	William Mitchell Chamberlain	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Negative	View
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Service Commission of South Carolina	Philip Riley	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Negative	
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Negative	View
10	Florida Reliability Coordinating Council	Linda Campbell		
10	Midwest Reliability Organization	Larry Brusseau	Negative	View
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council, Inc.	Edward A. Schwerdt		
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Negative	View
10	Southwest Power Pool	Charles H. Yeung	Negative	View
10	Western Electricity Coordinating Council	Louise McCarren	Negative	View

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on Initial Ballot — CIP-006-1 — Progress Energy Request for Interpretation (Project 2008-10)

Summary Consideration: There are five themes that emerged from the industry comments:

1) Wiring does not rely upon or utilize a routable protocol and thus cannot be a cyber asset any more than a power cable is. The NERC definition of cyber asset does not include the language "including the wiring that comprises the physical media supporting the network."

Response: The interpretation response team has reviewed its response and considers the wiring to be a component of the communication network, which is a cyber asset, as defined in the NERC Glossary. As such, the network wiring needs to be protected.

2) This is far too important to resolve via an interpretation. This needs to be addressed in the revisions to the CIP standards and subject to the full stakeholder process.

Response: We agree that this is an important issue, and it will be considered as part of the standards' revision in the Cyber Security Order 706 (CSO706) project (Project 2008-06). However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this request for interpretation (RFI) from Progress Energy.

3) The interpretation exceeds the process rules by changing the requirements of standard, adds concepts not consistent with other NERC guidance, speculates on the intent of the standard, and adds confusion and ambiguity with respect to compliance. It also opens the door for other non-physical "alternatives" to compliance with the requirements of CIP-006.

Response: While the drafting team disagrees it altered any requirements to the standard via the interpretation, the team acknowledges a lack of clarity regarding alternative measures. In drafting the revised interpretation, the team interprets the phrase "alternative measures" to include use of combined/complementary physical and logical approaches to achieve the same or better protection for Electronic Security Perimeter (ESP) wiring that is external to the Physical Security Perimeter (PSP).

4) The wire is not within the ESP; therefore it does not need to be protected. The wire is nothing more than a communication link specifically excluded by CIP-005, R1.3.

Response: The request clearly asked about wiring within an ESP.

5) The cost (dollars, time) to protect wiring in a campus setting far exceeds the benefit derived by doing so. The challenges of having to comply with all of the CIP-006 requirements are an impossible and unreasonable task. The decision to protect wiring should be based upon a proper risk determination process.

Response: The interpretation response team attempted to offer alternative methods for compliance without undue financial burden in the initial interpretation response. In drafting the revised interpretation, the team interprets the phrase "alternative measures" to include use of combined/complementary physical and logical approaches to achieve the same or better protection.

Entity	Segment	Vote	Comment
Allegheny Power	1	Negative	Allegheny Energy is concerned with the SAR drafting team interpretation that wiring within an ESP be considered a Cyber Asset or Critical Cyber Asset. Allegheny Energy agrees that the wiring (and information

Entity	Segment	Vote	Comment
			transmitted by such wiring) within an ESP needs to be protected; however, Allegheny Energy does not agree that the wiring needs to be classified and protected as a defined cyber asset. NERC defines cyber assets as programmable electronic devices and communication networks including hardware, software, and data and does not include the language “including the wiring that comprises the physical media supporting the network”. Allegheny Energy believes the best method to determine protection measures for the wiring (and information transmitted by such wiring) is to create a holistic approach to communication network and data communication link protection through the Standards process that specifically addresses these issues. This new Standard could address communication network and data communication link security issues, including copper cabling, fiber optic cabling, and wireless implementations. By the interpretation stating that network wiring is a cyber asset or potentially a critical cyber asset in an effort to physically secure the wiring, this statement would additionally impose all of the requirements of the CIP standard that are applicable to cyber assets and in essence make entities non-compliant since many requirements cannot be accomplished for wiring.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. For ESP wiring that is external to the PSP: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or monitoring to detect unauthorized access or physical tampering. The RFI response drafting team agrees that this is an important issue and it will be considered as part of the standards’ revision in the Cyber Security Order 706 (CSO706) project.			
Ameren Services Company	1	Negative	We do not agree with this interpretation. We feel that the language in the first sentence of the response, "including the wiring that comprises the physical media supporting the network," could be viewed to include aspects that are not covered in the CIP 002 - 009. Broad interpretation of the response would significantly impact the compliance burden. In addition, CIP 006 R1.1 states: "Where a completely enclosed (six-wall) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." This interpretation does not make it clear whether or not that part of the CIP-006 requirement 006 is still valid, and seems to supersede the CIP standard in this regard.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within			

Entity	Segment	Vote	Comment
an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
American Electric Power	1	Negative	Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue and it is presently being considered as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A methodology for determining the appropriate protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Associated Electric	1	Negative	Wiring meets none of the requirements of CIP-002-R3, the wiring does not communicate itself with anything, it is merely a communications conduit or channel, therefore the standard does not apply to it anymore than it

Entity	Segment	Vote	Comment
Cooperative, Inc.			would apply to the ac power wiring. While it is appropriate to protect access to all wiring inside the ESP, I do not believe that the intent of the standard is to consider wiring a CCA and subject it to all of the CIP requirements, many of which can not even be implemented or do not apply. These points were presented very well (and I am in complete agreement with) in the document by Mr. Tim Conway of NiSource, “Wiring as a CCA”.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Brazos Electric Power Cooperative, Inc.	1	Negative	Further clarity should be added to the last sentence to address the interpretation request as follows: Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures as it extends from the ESP up to the Physical Security Perimeter. Then there is the question about what is defined as "tampering".
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering. The RFI response drafting team views tampering to include, but is not limited to, unauthorized access, disruption, or alteration.			
Consolidated Edison Co. of New York	1	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.

Entity	Segment	Vote	Comment
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
FirstEnergy Energy Delivery	1	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that "Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The communication assets excluded from the standards are the Cyber Assets associated with communication networks and data communication links between			

Entity	Segment	Vote	Comment
discrete ESPs. There is no explicit reference within the standards to third-party communications. The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Hydro One Networks, Inc.	1	Negative	Hydro One Networks Inc. is casting a Negative vote with the following comment: The interpretation is not clear and may modify the intention of the Standard. It needs more work. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter," which must be protected. While the wires connecting two ESPs need to be protected it should not make one PSP of both. Appropriate conduit or similar protection as appropriate should be acceptable.
Response: The equipment configuration described in this comment wherein two physically separate Cyber Assets that are individually classified as having its own ESP would indeed not require physical access protection for the interconnecting wiring. However, the situation as described by the requestor is different. The configuration indicated by the requestor involves physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Manitoba Hydro	1	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that “the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network.” It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised RFI response. The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the			

Entity	Segment	Vote	Comment
drafting team disagrees with removal of the term communication network in the RFI response as it is already referenced in the NERC Glossary definition of a Critical Cyber Asset.			
National Grid	1	Negative	The interpretation is not clear and may modify the intention of the Standard. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures for ESP wiring that is external to the PSP may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
New Brunswick Power Transmission Corporation	1	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "…all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Orange and Rockland Utilities, Inc.	1	Negative	Orange and Rockland cannot support CIP-006 R1.1 and requests further clarification of "alternative protection measures" encompassing the wiring that comprises the "physical media" supporting the network.
Response: The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures for ESP wiring that is external to the PSP may include, but are not			

Entity	Segment	Vote	Comment
limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
Pacific Gas and Electric Company	1	Negative	As written the interpretation is too broad. The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within the pertinent parts of a given facility or campus.
Response: The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures for ESP wiring that is external to the PSP may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.			
PacifiCorp	1	Negative	"The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets "alternative measures" for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering. The drafting team believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected not to include such language.			
Potomac Electric	1	Negative	Pepco is a subsidiary of PHI. PHI feels that the interpretation is not clear and the response itself is subject to interpretation. This lack of clarity is the basis for PHI's rejection. PHI also believes that communication systems

Entity	Segment	Vote	Comment
Power Co.			should be protected. The Answer to Question 11 of the FAQ associated with these standards states that communication systems are not covered by these standards.

Response:

The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The asset owner is encouraged to reconsider the design of a communication network that extends the ESP across third-party communications systems and networks.

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

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

Question 11 of the FAQ for standard CIP-002-1 – Cyber Security – Critical Cyber Assets (reproduced below) refers to Section A 4.2.2 regarding the exclusion of Cyber Assets associated with communication networks and data communication links between discrete ESPs. Communications within the ESP are covered by these standards.

CIP-006-1 The asset owner is encouraged to reconsider the design of a communication network that extends the ESP across third-party communications systems and networks.

11. FAQ - Question: *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?*

Answer: Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset.

PP&L, Inc.	1	Negative	The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.

Response:

The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.

Entity	Segment	Vote	Comment
Puget Sound Energy, Inc.	1	Negative	Definition of Cyber Asset: We do not believe the existing definition of "Cyber Asset" should include wiring. From the most recent (February 12, 2008) NERC "Glossary of Terms Used in Reliability Standards": "Cyber Assets - Programmable electronic devices and communication networks including hardware, software, and data." Wires are not programmable, are not software, and are not data. While they are physical media, it is highly questionable if they could be considered hardware as our understanding is that hardware devices are what software runs on. If we were to extend the definition to include a wire strictly because it carries data, at what point do we consider a telephone pole a Cyber Asset because it carries wires which carry data? If the definition does include wiring, how then do wireless communications media fit into the definition in the context of physical protection of Cyber Assets? Wireless is neither hardware, software, or data and, with regards to this interpretation, physical protection of airborne electrons is not practical/possible with today's technology. Alternative Protective Measures: As most facilities which house Critical Cyber Assets were constructed prior to the CIP standard adoption by FERC, many such facilities have a common wiring infrastructure for both Critical Cyber Assets and assets that are not in scope for CIP compliance. We believe it is unreasonable to require every wire be traced and extracted from common conduit, cable bundles, or other common pathway for the purposes of re-enclosing them in a CIP-specific conduit or other “six-wall” perimeter. The very act of performing this work will introduce an increased reliability risk. If wiring is to be included in the definition of Cyber Asset, we feel that a “completely enclosed (“six-wall”) border” cannot be established for most wiring infrastructures given the above. Therefore, the "alternative measures to control physical access to the Critical Cyber Assets" phrase from CIP-006 R1.1 must be used. The definition for Critical Cyber Assets require that a Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, the Cyber Asset uses a routable protocol within a control center; or, the Cyber Asset is dial-up accessible, and wiring has no such attributes. Given that CIP-006 R1.1 talks about both Cyber Assets and Critical Cyber Assets, can the interpretation team comment on the above? We would also like clarification on whether "alternative protective measures" includes situations that only deploy purely logical controls of data transiting the wire. As the interpretation team has stated, “The intent is to protect the data transmitted over the network within the ESP”, would an ESP that spans an entity’s entire infrastructure and only employs logical “alternative protective measures”, be an acceptable response to this interpretation? Summary: We commend the interpretation team for wanting to address data in motion, but the appropriate venue to address this issue is NERC Project 2008-06 as CIP-006 R1.1 prescribes requirements for physical protection of Cyber Assets (or just Critical Cyber Assets when a “six-wall” perimeter cannot be established) within an ESP. Additionally, based on our assessment of the term Cyber Asset, we believe requirements to protect communications media are beyond the scope of the existing CIPs. Outstanding RFI How does the Project 2008-10 interpretation for Progress Energy relate to the previous interpretation request (below) from October 10, 2007 by Puget Sound Energy? --- 1) We are requesting an interpretation of the term “externally connected” as used in 005.R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s) We request an interpretation which allows encrypted connections over frame relay within a single ESP. Note in the diagram above the routers are not considered “access points” to the ESP, but rather are contained within it. 2) We are requesting clarification of CIP-006-1 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

Entity	Segment	Vote	Comment
			enclosed ("six wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets. The standard does not explicitly require a given ESP to be fully contained by a single PSP. We request a clarifying interpretation which allows an ESP to span multiple PSPs provided that communications within the ESP are protected sufficiently to prevent unauthorized access. Commentary: With the use of encrypted tunnels and physical protection of the tunnel endpoints, we believe that secure, CIPS compliant ESPs can be designed which span multiple PSPs. It should be noted that 005.R1.3 defines communication links between ESPs as an "access point", which in turn requires port/protocol restrictions at the access point (005.R2.2). However, OSI layer 3 controls won't solve what is fundamentally an OSI layer 2 concern. Specifically, port and protocol restrictions at the endpoints of a frame relay connection will not adequately mitigate the risk of exposure to packets being manipulated at OSI Layer 2. Hence, our desire to use encrypted tunnels to assure packet integrity and source authenticity thereby addressing the layer 2 concerns. Thank you for the opportunity to comment.
Response: The RFI response team agrees with the comment that the main objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. In regard to wiring, the RFI response drafting team asserts that the definition of Cyber Asset in the NERC Glossary indeed includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. With respect to the commentary about a single ESP spanning multiple PSPs, the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 applies. The drafting team is not familiar with the October 10, 2007 RFI by Puget Sound Energy.			
Salt River Project	1	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat.
Response:			

Entity	Segment	Vote	Comment
The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Seattle City Light	1	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.

Response:

The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.

The scenario described in this comment wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring.

The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection.

The recommendation to address data in motion is currently included in the work of the CSO706 Project.

Entity	Segment	Vote	Comment
Sierra Pacific Power Co.	1	Negative	This interpretation seems to expand the applicability of the CIP Requirements outside the bounds of the Critical Assets.
Response: The RFI response drafting team does not expand the applicability of the CIP requirements but states the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			
Southern California Edison Co.	1	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team's proposed interpretation for CIP-006-1's Requirement 1.1 ("Proposed Interpretation"). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that "Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." SCE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE's communications network, and the data which streams across it, is strictly controlled by an Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rites dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that			

Entity	Segment	Vote	Comment
is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, the request from Progress Energy must be addressed in the formal Interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Southern Company Services, Inc.	1	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The phrase "alternative measures" in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Southwest Transmission Cooperative, Inc.	1	Negative	"The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response:			

Entity	Segment	Vote	Comment
The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team believes alternative measures is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible.			
Tampa Electric Co.	1	Negative	Tampa Electric Company’s Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry’s attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security “ such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.

Entity	Segment	Vote	Comment
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Tennessee Valley Authority	1	Negative	While we agree that physical and electronic perimeters must be the same or the data must protected as it traverses physical perimeters, TVA doesn't think that the interpretation provides sufficient detail to guide compliance.
Response: The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team is limited in its ability to provide more explicit guidance and believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tucson Electric Power Co.	1	Negative	TEP supports the following provided by WECC: "The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to			

Entity	Segment	Vote	Comment
avoid such language.			
Westar Energy	1	Negative	Disagree with the concept that wire is a Cyber Asset.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			
Western Area Power Administration	1	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to "wires within a given facility or campus" and therefore doing so is unjustified. The drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Xcel Energy, Inc.	1	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on

Entity	Segment	Vote	Comment
			entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope. The team understands the desire for more specificity and prescription such as in a diagram but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
British Columbia Transmission Corporation	2	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
California ISO	2	Negative	The interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with “what should have been done”. The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address. Conflicts: the interpretation crosses multiple standards CIP-006-1, 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-005-1, R1.3: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)."

Entity	Segment	Vote	Comment
			Glossary: "Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data." The reference in CIP-005, R1.3 describes "communication links"; in reality, those links are the "wiring" that the interpretation request is describing; thus, they are not within the Electronic Security Perimeter and do not need to be within a Physical Security perimeter.
Response: The RFI response drafting team recognizes that while data in transit is fundamentally the asset to be protected, it agrees that the CSO706 Project is where it should be addressed. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Independent Electricity System Operator	2	Negative	Although directionally the IESO is in favour of the intent of the interpretation, we believe the current interpretation wording may effectively modify the intention of the standard, which is inconsistent with NERC standard development protocol, and hence the interpretation needs more work. CIP-006-1, R1.1 states: "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(emphasis added) to the Critical Cyber Assets." the interpretation states: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring OR ALTERNATIVE PROTECTIVE MEASURES(emphasis added). Whereas the standard clearly requires physical access control, the interpretation effectively relaxes this requirement with the words either through physical protection of the wiring or alternate protective measures where the resultant implication is that the alternate protective measures are non-physical, hence a relaxation of the standard. Although we believe the standard should be revised to allow alternative protective measures, that is not the issue being balloted.
Response: The RFI response drafting team respectfully disagrees that the scope of alternative measures does not include logical approaches. The drafting team concurs that the intent is to protect the data that travels over the wiring and asserts that either physical or logical measures are capable of achieving the desired objective.			
ISO New England, Inc.	2	Negative	There are three significant issues with this Interpretation which resulted in a negative vote: (1) the interpretation adds requirements that are not already part of the Standard, the Standard intentionally did not originally address data in transit over communication links; (2)the interpretation creates conflicts between CIP-006 R1.1 and CIP-005, R1.3, which clearly states that communication links connecting discrete ESPs shall not be considered part of the ESP; and (3) we believe that the current Standard is clear enough and this interpretation simply creates more confusion in the industry, we have not had any problems in understanding or implementing

Entity	Segment	Vote	Comment
			the Requirements in this Standard.
Response: (1) The notion of data in transit, while at the core of the protection purpose, is more appropriately addressed in the ongoing CSO706 Project. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. (2) Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP. (3) The drafting team is compelled by process to respond to this RFI from Progress Energy.			
Midwest ISO, Inc.	2	Negative	The FAQ developed along with the original CIP standards specifically state that the standards are not intended to address the wires between facilities. While we agree that the suggested interpretation is a good idea for a future improvement to the standard, the interpretation process is intended to clarify what the standard says as originally drafted, not what we would like the standard to say.
Response: The FAQ is a guidance document and is not mandatory and enforceable as NERC standards are. However, question #11 (reproduced below) refers to assets that are not owned by the Responsible Entity, such as third party telecommunications company equipment. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. In this instance, the wiring referenced by Progress Energy is clearly within a single ESP. **11. FAQ - Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?* **Answer:** Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset.			
PJM Interconnection, L.L.C.	2	Negative	PJM has the following concerns: Procedural: the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address. Conflicts: the interpretation crosses multiple standards CIP-006-1, 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-005-1, R1.3: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)." Glossary: "Cyber Assets: Programmable

Entity	Segment	Vote	Comment
			electronic devices and communication networks including hardware, software, and data." The reference in CIP-005, R1.3 describes "communication links"; in reality, those links are the "wiring" that the interpretation request is describing; thus, they are not within the Electronic Security Perimeter and do not need to be within a Physical Security perimeter. Necessity: the definitions and descriptions contained within the published standard seem clear; the issue has posed no significant problems for SWG member organizations to understand or implement.
Response: The RFI response drafting team recognizes that while data in transit is fundamentally the asset to be protected, it agrees that the CSO706 Project is where it should be addressed. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Alabama Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
American Electric Power	3	Negative	Although we agree that a true "systems" approach to data protection would also include the data paths, we are concerned about an element that we believe should be included in any determination of communication path physical security. Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively

Entity	Segment	Vote	Comment
			accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Consolidated Edison Co. of New York	3	Negative	The interpretation is not clear, may modify the intention of the Standard, and needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Consumers Energy	3	Negative	Consumers Energy’s understanding of the requirements of CIPS-005-1 and CIPS-006-1 as they were being developed and as they exist today allowed for discrete non-contiguous physical security perimeters to protect cyber assets contained within a single electronic security perimeter, presumably by excluding the communication network and data passing over the communication network as being defined as Cyber Assets requiring physical protection. We believe that this view is consistent with good utility practice utilized at a number of North America’s control centers and generating plants. In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the original drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems or devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, and none of the nine requirements specifically address network cables or data. Had the original intent of the standards been to include the communication networks within an electronic security perimeter as Cyber Assets requiring physical protection we would have expected the standard to address appropriate protection where six-wall physical protection (complete with access control

Entity	Segment	Vote	Comment
			and monitoring) is not necessary (such as with buried portions of the network) or practical (such as within raceways or conduit). Additionally, the time required to re-wire such networks so as to provide six-wall physical protection is significantly longer than the time required to provide six-wall physical protection to the access points to Cyber Assets within the Electronic Security Perimeter. Further, had the original intent of the standards been to include data that passes over the communication network, the standard should have discussed the issues associated with transporting, storing and restoring back-up tapes and other removable media so as to protect cyber assets in the event the back-up data is re-introduced to the electronic security perimeter. We suggest the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. We believe the primary intent of the present version of the CIP Standards is to protect against remote compromise of those assets. The apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards as they were developed and implemented. CIP-006-1 R1.1 states "ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter." This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting communication network cabling residing in an area entirely within the reasonable and prudent control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all communication network and data as Cyber Assets requiring physical protection, the wording should have stated such. If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between "in-house" cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. We propose the following wording to replace the existing interpretation: Response: The Physical Security Perimeter is required to protect the access points to Critical Cyber Assets within the Electronic Security Perimeter. For dedicated communication networks within a discrete Electronic Security Perimeter under the normal reasonable and prudent control of the Responsible Entity, all elements of such network do not require to be contained within the Physical Security Perimeter so long as all access points to the Critical Cyber Assets within the Electronic Security Perimeter are also within a Physical Security Perimeter. CIP-005-1 R1.1 refers to any externally connected communication end point (for example, dial-up modems) as specifically identified as an access point to the Electronic Security Perimeter. The use of "externally connected" in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be "external" would include local area networks between floors in a building or between buildings in a campus environment.
Response: The RFI response drafting team believes the commenter's presumption that protection is not required for wiring between "discrete non-contiguous physical security perimeters" is not justified. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a			

Entity	Segment	Vote	Comment
single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP. The drafting team believes that the other concerns raised by the commenter, including transfer of backup tapes and other removable media, is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project.			
Cowlitz County PUD	3	Negative	Cowlitz County PUD No.1 (District) finds the interpretation does not clarify the intent of the Standard. Extension of the "6-wall" physical security perimeter with conduit would require an accounting for all access points (condulets or conduit bodies) and appropriate access monitoring. Simple use of conduit does not offer the best protection of data as it can be easily compromised. The verbiage "or alternative protective measures" needs clarification - or alternative physical and/or logical protective measures - to protect the original intent of the Standard. The District's position is that logical protective measures (such as loss of continuity alarms) will in many cases better protect data from malicious tampering than physical protective measures.
Response: The RFI response drafting team clarifies CIP-006 R1.1 which states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Duke Energy Carolina	3	Negative	Thank you for the opportunity to vote on this interpretation. We think that the interpretation is unclear. A new NERC Cyber Security drafting team is in the process of being assembled, and Duke Energy believes that this issue is best addressed in a comprehensive manner by the new Cyber Security drafting team. The manner of protecting data from tampering when it is transmitted over networks should be clearly defined in the new Cyber Security Standard, and any newly prescribed protection methods must be properly related to other requirements in the standards where that is appropriate.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			

Entity	Segment	Vote	Comment
FirstEnergy Solutions	3	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that ""Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Georgia Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. -

Entity	Segment	Vote	Comment
			The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Gulf Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Hydro One Networks, Inc.	3	Negative	Hydro One Networks Inc. is casting a Negative vote with the following comment: The interpretation is not clear and may modify the intention of the Standard. It needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter," which must be protected. While the wires connecting two ESPs need to be protected it should not make one PSP of both. Appropriate conduit or similar protection as appropriate should be acceptable.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the			

Entity	Segment	Vote	Comment
connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. Appropriate conduit, as suggested by the commenter, is an acceptable physical protection.			
Lincoln Electric System	3	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 applies.			
Madison Gas and Electric Co.	3	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the

Entity	Segment	Vote	Comment
			explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal Interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team disagrees with the commenter that the exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Manitoba Hydro	3	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			

Entity	Segment	Vote	Comment
However, the drafting team disagrees with removal of the term communication network in the RFI response as it already referenced in the NERC Glossary.			
MidAmerican Energy Co.	3	Negative	MidAmerican Energy believes that this interpretation expands the requirements of the standard inappropriately.
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Mississippi Power	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-1 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
New York Power Authority	3	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "... all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimieter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a			

Entity	Segment	Vote	Comment
completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Niagara Mohawk (National Grid Company)	3	Negative	The interpretation is not clear and may modify the intention of the Standard and therefore needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimieter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Platte River Power Authority	3	Negative	The interpretation would be acceptable if language is added similar to what is suggested below: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering. Where (“six-wall”) physical protection of the wiring cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to			

Entity	Segment	Vote	Comment
physical tampering.			
Public Utility District No. 2 of Grant County	3	Affirmative	
Salt River Project	3	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat.
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Seattle City Light	3	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.
Response: The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			

Entity	Segment	Vote	Comment
The scenario described by the commenter wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection. The recommendation to address data in motion is currently included in the work of the CSO706 Project.			
Tampa Electric Co.	3	Negative	Tampa Electric Company’s Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry’s attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: • These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. • The primary DCS vendors in our environment do not offer or support an approved mechanism for encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. • The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective

Entity	Segment	Vote	Comment
			based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: • Unauthorized access to the ESP through access to physical cabling. • Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. • Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.			
Wisconsin Public Service Corp.	3	Negative	The interpretation for CIP-006 significantly expands the scope of the standard and needs to go through through the SAR process. The inclusion of communications network wiring is a shift from previous industry understanding and is contrary to responses for Frequently Asked Questions posted on the NERC website. Standard CIP-002-1 — Cyber Security — Critical Cyber Assets 11. Question: Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards? Answer: Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset. Standard CIP-005-1 Cyber Security — Electronic Security 2. Question: I am connected to other partners Electronic Security Perimeters through a Wide Area Network (WAN) connection. What is now included in the Electronic Security Perimeter? Is the connection to the partner included? Answer: The standard states that where discrete Electronic Security Perimeters are connected by communication lines, the communication lines are not included in the Electronic Security Perimeter. 15. Question: Is a physically isolated and dedicated network required for connections between Electronic Security Perimeters? Answer: No, physical isolation is not required, nor is a dedicated link required. The standard does not specify any requirement for communication between discrete Electronic Security Perimeters, since this is currently beyond the scope of these standards. It

Entity	Segment	Vote	Comment
			is possible for the data between discrete perimeters to be carried over a shared infrastructure such as a shared WAN, or to be carried over dedicated links. However, the Responsible Entity must ensure that the access control devices (such as firewalls) at the access points to the Electronic Security Perimeters do not permit unauthorized access to the Electronic Security Perimeters and the Cyber Assets within them. When data is carried over a shared infrastructure, the Responsible Entity should ensure as well that the data has not been changed in transit. Logical or virtual separation of the data in a shared infrastructure can be accomplished by using existing technologies such as virtual circuits and communication tunnels. Encryption or other data integrity checking technologies can also ensure that data is not changed in transit, provided performance and latency requirements for the applications are satisfied. Standard CIP-006-1 — Cyber Security — Physical Security 20. Question: Does the standard require entities to protect telecommunications services and facilities that serve physical security system assets? Answer: CIP-002 through CIP-009 do not address telecommunications.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. The RFI response team clarifies in a revised interpretation response that physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. Protection of communication systems that reside within an ESP is required. The Frequently Asked Questions posted on the NERC website is a guidance document and is not mandatory and enforceable as NERC standards are. However, question #11 (reproduced below) refers to assets that are not owned by the Responsible Entity such as third-party telecommunications company equipment. **11. FAQ - Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?* **Answer:** Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset. In addition, the figure associated with Question 2 for CIP-005-1 (Page 12 of the FAQ) specifically addresses the commenter's concerns regarding interconnectivity of ESP's over Wide Area Networks. This interpretation does not change the exclusion of communication networks outside of an ESP from the standard. In this instance the wiring is clearly stated by Progress Energy to be within a single ESP.			
Xcel Energy, Inc.	3	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these

Entity	Segment	Vote	Comment
			rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Alliant Energy Corp. Services, Inc.	4	Negative	CIP-005 - R1.3 specifically excludes the connecting cabling from the CIP standards. There can not be such conflicting statements between standards.
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Consumers Energy	4	Negative	Consumers Energy's understanding of the requirements of CIPS-005-1 and CIPS-006-1 as they were being developed and as they exist today allowed for discrete non-contiguous physical security perimeters to protect cyber assets contained within a single electronic security perimeter, presumably by excluding the communication network and data passing over the communication network as being defined as Cyber Assets requiring physical protection. We believe that this view is consistent with good utility practice utilized at a number of North America's control centers and generating plants. In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the original drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems or devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, and none of the nine requirements specifically address network cables or data. Had the original intent of the standards been to include the communication networks within an electronic security perimeter as Cyber Assets requiring physical protection we would have expected the standard to address appropriate protection where six-wall physical protection (complete with access control and monitoring) is not necessary (such as with buried portions of the network) or practical (such as within raceways or conduit). Additionally, the time required to re-wire such networks so as to provide six-wall physical protection is significantly longer than the time required to provide six-wall physical protection to the access points to Cyber Assets within the Electronic Security Perimeter. Further, had the original intent of the standards been to include data that passes over the communication network, the standard should have discussed the issues associated with transporting, storing and restoring back-up tapes and other removable media so as to protect cyber assets in the event the back-up data is re-introduced to the electronic security perimeter. We

Entity	Segment	Vote	Comment
			suggest the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. We believe the primary intent of the present version of the CIP Standards is to protect against remote compromise of those assets. The apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards as they were developed and implemented. CIP-006-1 R1.1 states "ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter." This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting communication network cabling residing in an area entirely within the reasonable and prudent control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all communication network and data as Cyber Assets requiring physical protection, the wording should have stated such. If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between "in-house" cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. We propose the following wording to replace the existing interpretation: Response: The Physical Security Perimeter is required to protect the access points to Critical Cyber Assets within the Electronic Security Perimeter. For dedicated communication networks within a discrete Electronic Security Perimeter under the normal reasonable and prudent control of the Responsible Entity, all elements of such network do not require to be contained within the Physical Security Perimeter so long as all access points to the Critical Cyber Assets within the Electronic Security Perimeter are also within a Physical Security Perimeter. CIP-005-1 R1.1 refers to " any externally connected communication end point (for example, dial-up modems) " as specifically identified as an access point to the Electronic Security Perimeter. The use of "externally connected" in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be "external" would include local area networks between floors in a building or between buildings in a campus environment.

Response:

The RFI response drafting team believes the commenter's presumption that protection is not required for wiring between "discrete non-contiguous physical security perimeters" is not justified. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies.

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

Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.

Entity	Segment	Vote	Comment
The drafting team believes that the other concerns raised by the commenter, including transfer of backup tapes and other removable media, is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project.			
Madison Gas and Electric Co.	4	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team disagrees with the commenter that exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-			

Entity	Segment	Vote	Comment
006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Seattle City Light	4	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.
Response: The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006. The scenario described by the commenter wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection. The recommendation to address data in motion is currently included in the work of the CSO706 Project.			

Entity	Segment	Vote	Comment
Seminole Electric Cooperative, Inc.	4	Negative	Seminole endorses the comments of Tampa Electric Company as replicated below: Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. We have several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach my be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment do not offer or support an approved mechanism for encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, we recommend that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.

Response:

The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden.

Entity	Segment	Vote	Comment
However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Wisconsin Energy Corp.	4	Negative	Interpetation is overreaching
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
WPS Resources Corp.	4	Negative	The interpretation for CIP-006 significantly expands the scope of the standard and needs to go through through the SAR process. The inclusion of communications network wiring is a shift from previous industry understanding and is contrary to responses for Frequently Asked Questions posted on the NERC website.
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
AEP Service Corp.	5	Negative	Although we agree that a true "systems" approach to data protection would also include the data paths, we are concerned about an element that we believe should be included in any determination of communication path physical security. Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or inobtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response:			

Entity	Segment	Vote	Comment
The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Allegheny Energy Supply Company, LLC	5	Negative	Allegheny Energy is concerned with the SAR drafting team interpretation that wiring within an ESP be considered a Cyber Asset or Critical Cyber Asset. Allegheny Energy agrees that the wiring (and information transmitted by such wiring) within an ESP needs to be protected; however, Allegheny Energy does not agree that the wiring needs to be classified and protected as a defined cyber asset. NERC defines cyber assets as programmable electronic devices and communication networks including hardware, software, and data and does not include the language “including the wiring that comprises the physical media supporting the network”. Allegheny Energy believes the best method to determine protection measures for the wiring (and information transmitted by such wiring) is to create a holistic approach to communication network and data communication link protection through the Standards process that specifically addresses these issues. This new Standard could address communication network and data communication link security issues, including copper cabling, fiber optic cabling, and wireless implementations. By the interpretation stating that network wiring is a cyber asset or potentially a critical cyber asset in an effort to physically secure the wiring, this statement would additionally impose all of the requirements of the CIP standard that are applicable to cyber assets and in essence make entities non-compliant since many requirements cannot be accomplished for wiring.
Response: The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. As such the RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
City of Tallahassee	5	Negative	CIP-005-1, R1.3 states: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)."

Entity	Segment	Vote	Comment
			Since it is not within the Electronic Security Perimeter, it does NOT need to be within a Physical Security perimeter that is required in CIP-006-1, R1.1. (Glossary) Cyber Assets: "Programmable electronic devices and communication networks including hardware, software, and data." I disagree that this includes the "wires". The "communication links connecting" are the "wires" and they are excluded per CIP-005, R1.3. We cannot have one standard saying the wires are included and another saying they are not!
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Colmac Clarion/Piney Creek LP	5	Affirmative	Appears to adequately require either 'six boundary' enclosure or entity description of protective measures on wiring or components outside of same. Doesn't require that entity methods equal six wall protection however.
Response: Thank you for your comment. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Consumers Energy	5	Negative	Consumers Energy’s Comments to Accompany a “No” Vote on NERC 2008-10 August 6, 2008 **2008-10 Goes Beyond the Intent of the Standards** In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems, devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, not network cables or data. **Data and Cables Would Become Critical Cyber Assets** If this interpretation passes, network cables and data will be considered Cyber Assets. Since it is difficult to conceive of an Asset that uses a network where data and networks are not essential to the operation of that Asset, data and network cabling will become Critical Cyber Assets. This will be true for control centers, generating plants and substations. **Data as a Critical Cyber Asset** The act of identifying data as a Critical Cyber Asset has far-reaching implications. Will removable media such as backup tapes need to be stored within an Electronic Security Perimeter? How can media so protected be

Entity	Segment	Vote	Comment
			moved to an off-site storage location? **Actual Intent - Cyber Asset Has CPU** Consumers Energy suggests the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. Consumers Energy further suggests the primary intent of the present version of the CIP Standards is to protect against remote compromise. **Intent of Interpretation Goes Too Far for This Stage** Consumers Energy also suggests that the apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards in their present form. CIP-006-1 R1.1 states “ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.” This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting network cabling residing in an area entirely within the control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all connections outside the ESP, the wording should have stated such. Threats and Priorities If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between “in-house” cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. **Proposed Rewording** Consumers Energy proposes the following wording to replace the existing interpretation: Response: CIP-006-1 R1.1 refers to “any externally connected communication end point (for example, dial-up modems)” as specifically identified as an access point to the Electronic Security Perimeter. The use of “externally connected” in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be ”external” would include local area networks between floors in a building or between buildings in a campus environment.

Response:

On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.

The RFI response drafting team agrees and acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also notes that Critical Cyber Asset classification is an important issue and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. Therefore, the

Entity	Segment	Vote	Comment
matter of data protection is not directly address by this RFI response. The drafting team does not agree that protection of only Cyber Assets with CPUs is the intent of the CIP standards. The drafting team believes that the requirement clearly states that “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team appreciates the suggested replacement wording, but believes it does not meet the objective of CIP-006-1.			
Detroit Edison Company	5	Negative	The following are Detroit Edison's reasons for voting No: The NERC Glossary defines Cyber Assets as “Programmable electronic devices and communication networks including hardware, software, and data”. Detroit Edison believes that this definition relating to the network is to include active devices that comprise the network, not the transmission media itself. Thus routers, switches, hubs, etc. are cyber assets, wiring is not. Detroit Edison's opinion on protecting cabling between physical security perimeters fully contained within an otherwise adequately secured facility is that the cable is sufficiently protected following guidance provided by NIST. Additional protection can be provided by covering the cable trays where they are easily accessible. "NIST SP800-53 PE-4 Access Control For Transmission Medium, Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays." Note that conduit and cable tray is specified as adequate protection by NIST however, if the interpretation is approved as written a completely enclosed six wall boundary would be required. Does this mean that all conduit bodies, pull boxes, cable tray covers, and open cable trays would become access points subject to CIP-006? "FERC Order 706 paragraph 224: Congressional Representatives state that NIST research prepared a technical report comparing the proposed CIP Reliability Standards with SP 800-53. This technical report found that an organization conforming to the baseline set of security controls in SP 800-53 will also comply with the management, operational and technical security requirements of the CIP Reliability Standards, though the converse may not be true." Detroit Edison believes that the outer barrier cable jacket, designed and manufactured to protect the data transport media within the jacket, represents a comprehensive six wall cable barrier and furthermore, completely enclosing wiring between physical security perimeters with a second protective measure such as a conduit, would be unduly burdensome, increase the risk of creating adjacency hazards and would not significantly improve the security posture of the critical cyber assets in the electronic security perimeter. Detroit Edison further supports the use of alternative protective measures such as data encryption where technically feasible, over the use of conduit,

Entity	Segment	Vote	Comment
			which significantly provides enhanced security over the use of conduit alone.
Response: On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The examples of cable protection cited in the comment appear to be viable physical approaches; however, the conclusion that a six-wall bounded physical solution is the only acceptable one is not accurate. The Requirement R1.1 of CIP-006-1 clearly states that “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
FirstEnergy Solutions	5	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that “Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter.			

Entity	Segment	Vote	Comment
The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Lincoln Electric System	5	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: Thank you for your comment. The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Manitoba Hydro	5	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the drafting team disagrees with removal of the term communication network in the RFI response, as it already referenced in the NERC Glossary.			

Entity	Segment	Vote	Comment
Northern States Power Co.	5	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Pacific Gas and Electric Company	5	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” i not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			

Entity	Segment	Vote	Comment
PPL Generation LLC	5	Negative	Response: The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.
Response: The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.			
Reliant Energy Services	5	Negative	Reliant Energy is in agreement with the following comment posted by First Energy at 3:54 pm on August 13, on PJM’ NERC Standard e-Room. That is; “he definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly; the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team agrees that protection can be provided through alternative measures that include use of a combined/complementary physical and logical approach to achieve the same or better protection.			
Salt River Project	5	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			

Entity	Segment	Vote	Comment
Southern California Edison Co.	5	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team' proposed interpretation for CIP-006-1's Requirement 1.1 (Proposed Interpretation). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." CE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE's communications network, and the data which streams across it, is strictly controlled by an Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rights dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.

Response:

The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.

However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.

The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current

Entity	Segment	Vote	Comment
Requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tampa Electric Co.	5	Negative	Tampa Electric Company's Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: • These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. • The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. • The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations. We believe

Entity	Segment	Vote	Comment
			that the Standard Authorization Request should be modified to address concerns and issues related to: • Unauthorized access to the ESP through access to physical cabling. • Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Tennessee Valley Authority	5	Negative	The factors, which lead to this conclusion, are the exponential increase in scope and cost for the implementation of physical security applied to the communication media.
Response: CIP-006-1 requires all Cyber Assets within an ESP to be enclosed within a PSP. The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden.			
U.S. Bureau of Reclamation	5	Negative	This issue raises a question as to the NERC requirements for the physical protection of critical cyber assets that fall outside of readily defined Physical Security Perimeters (PSPs). The connection between the two PSPs is a communications line employing a routable protocol and may be based on microwave, radio, copper, or fiber technologies. For circuits that go between physical structures separated by more than several feet, the 6 wall requirement is impractical. NERC's response to the question raised was consistent with their overall requirements in the sense that they did not relax protection requirements for Critical Cyber Assets (specifically wiring) external to an Electronic Security Perimeter (ESP). Reclamation will be significantly impacted by this interpretation for its Critical Cyber Systems that extend over several physical sites. Specifically in cases where those sites are interconnected with communications circuits employing "routable protocols." In those instances, since physical protection of the circuits will be impractical or impossible, Reclamation will need to employ "alternate protective measures" on communications lines interconnecting the physically distinct sites. We suggest NERC reconsider their requirements in cases where interconnections between sites remain within the same "control system" and where those interconnections are carried over privately owned circuits. The

Entity	Segment	Vote	Comment
			requirements NERC has outlined make very good sense (and we support them) where the connections go to external entities or where they are carried over public networks. We have no desire to change this aspect of the requirements. We are requesting special consideration be given to private networks between physical and electronic perimeters where those networks are owned/operated by the entities in question.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. The RFI response team is limited to interpreting the requirement of the existing standard. The request for consideration of private networks is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.			
AEP Marketing	6	Negative	Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Consolidated Edison Co. of New York	6	Negative	The interpretation is not clear and may modify the intention of the Standard and needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring			

Entity	Segment	Vote	Comment
needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
FirstEnergy Solutions	6	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple			

Entity	Segment	Vote	Comment
physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Lincoln Electric System	6	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: Thank you for your comment. The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Madison Gas and Electric Co.	6	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?

Entity	Segment	Vote	Comment
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team disagrees with the commenter that exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Manitoba Hydro	6	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the drafting team disagrees with removal of the term communication network in the RFI response, as it already referenced in the NERC Glossary.			
PP&L, Inc.	6	Negative	Response: The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The

Entity	Segment	Vote	Comment
			intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.
Response: The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.			
Salt River Project	6	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Southern California Edison Co.	6	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team’s proposed interpretation for CIP-006-1’s Requirement 1.1 (Proposed Interpretation). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that “Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network.” SCE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE’s communications network, and the data which streams across it, is strictly controlled by an

Entity	Segment	Vote	Comment
			Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rights dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current Requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tampa Electric Co.	6	Negative	Tampa Electric Company's Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level

Entity	Segment	Vote	Comment
			of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Xcel Energy, Inc.	6	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could

Entity	Segment	Vote	Comment
			still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
California Energy Commission	9	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to "wires within a given facility or campus" and therefore doing so is unjustified. The drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Commonwealth of Massachusetts Department of Public Utilities	9	Negative	The interpretation should not include speculation as to the intent of the reliability standard.
Response:			

Entity	Segment	Vote	Comment
The RFI response drafting team does not speculate but rather interprets the standard as permitting "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Oregon Public Utility Commission	9	Negative	The interpretation should not include speculation as to the intent of the standard. The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response drafting team does not speculate but rather interprets the standard as permitting "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering. The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response, and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset and would thus not qualify in and of itself as a Critical Cyber Asset. The drafting team believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Electric Reliability Council of Texas, Inc.	10	Negative	This interpretation is an issue that should be handled through the full Standard review process.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is			

Entity	Segment	Vote	Comment
among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Midwest Reliability Organization	10	Negative	MRO Response: CIP-005-1, R1.3 states: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)." Since it is not within the Electronic Security Perimeter, it does NOT need to be within a Physical Security perimeter that is required in CIP-006-1, R1.1. (Glossary) Cyber Assets: "Programmable electronic devices and communication networks including hardware, software, and data." The MRO disagrees that this includes the "wires". The "communication links connecting" are the "wires" and they are excluded per CIP-005, R1.3. We cannot have one standard saying the wires are included and another saying they are not!
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
SERC Reliability Corporation	10	Negative	The interpretation indicates that the definition of a Cyber Asset includes the wiring that comprises the physical media supporting the [communications] network -- although this is not included in the NERC Glossary definition. The interpretation goes on to state that the intent is to protect the “data” transmitted over the network within the Electronic Security Perimeter rather than to protect “the facilities, systems, and equipment which if destroyed, degraded, compromised or otherwise rendered unavailable, would affect the reliability of the Bulk Electric System as a whole, not risk to a Responsible Entity’s individual asset” as described in Security Guidelines for the Electric Sector: Identifying Critical Assets. The interpretation merely restates the requirement of CIP-006-1, R1.1 to take (either Physical Security Perimeter or alternative) measures to control physical access of Critical Cyber Assets and adds confusion to the standard by introducing concepts contrary to other reference material provided by NERC.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			

Entity	Segment	Vote	Comment
Southwest Power Pool	10	Negative	SPP believes the concerns raised in this interpretation are too important to let lie in an interpretation. Although the interpretation provides additional guidance about the intent of the standard, it is not good practice to keep the requirement as written. A rewrite of R1.1 under a clear scope is a better way for the industry to understand the intent.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Western Electricity Coordinating Council	10	Negative	“The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus.” “If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.”
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets
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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the Cyber Security Order 706 SAR drafting team in response to industry comments received from the initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:
The definition of Cyber Asset in the *NERC Glossary of Terms Used in Reliability Standards* includes communication networks. Physical media (wiring) is a component of a communication network within an Electronic Security Perimeter, but the wiring itself is not a separate Cyber Asset.

The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the Electronic Security Perimeter. Since the connective wiring is inside the Electronic Security Perimeter, Requirement R1.1 of CIP-006-1 applies.

CIP-006-1 R1.1 also provides: "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." For wiring within the Electronic Security Perimeter that is external to a Physical Security Perimeter, the alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to data encryption, and/or circuit monitoring to detect unauthorized access or physical tampering.

From: Crews, David [mailto:david.crews@pgnmail.com]
Sent: Wednesday, April 02, 2008 5:05 PM
To: Gerry Adamski
Cc: Woods, Bruce; Goff, Edwin
Subject: Request for Interpretation CIP Standard

Progress Energy requests a formal interpretation of **CIP-006-1.** R1.1.

In **CIP_006-1**, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In **CIP-005-1,** Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In **CIP-002-1,** Requirement 3 states **"**Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

> **R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> **R3.2.** The Cyber Asset uses a routable protocol within a control center; or,
>
> **R3.3.** The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Initial Ballot Window Open

September 30–October 12, 2009

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

Project 2008-10: Interpretation for CIP-006-1 Requirement R1.1 for Progress Energy
An initial ballot window for a revised interpretation of standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 for Progress Energy is now open **until 8 p.m. EDT on October 12, 2009**.

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

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

Project Background:
Progress Energy asked if electronic security perimeter wiring external to a physical security perimeter must be protected within a six-wall boundary. The team has revised the interpretation based on stakeholder comments submitted during the initial ballot for the first draft of the interpretation.

The request and interpretation can be found on the project page:
http://www.nerc.com/filez/standards/Project2008-10_CIP-006_Interpretation_Progress.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 Pool and Pre-ballot Window
August 31–September 30, 2009

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

Project 2008-10: Interpretation for CIP-006-1 Requirement R1.1 for Progress Energy

A revised interpretation of standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 for Progress Energy is posted for a 30-day pre-ballot review. Registered Ballot Body members may join the ballot pool to be eligible to vote on this interpretation **until 8 a.m. EDT on September 30, 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-2008-10_RFI_PE_Rev1_in.

Next Steps

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

Project Background

Progress Energy asked if electronic security perimeter wiring external to a physical security perimeter must be protected within a six-wall boundary. The team has revised the interpretation based on stakeholder comments submitted during the initial ballot for the first draft of the interpretation.

The request and interpretation can be found on the project page:
http://www.nerc.com/filez/standards/Project2008-10_CIP-006_Interpretation_Progress.html

Standards Development Process

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Initial Ballot Results

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

Project 2008-10: Interpretation of CIP-006-1 for Progress Energy
The initial ballot for a revised interpretation of standard CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 for Progress Energy ended on October 12, 2009.

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

Quorum: 79.92%
Approval: 74.47%

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

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

Project Background
Progress Energy asked if Electronic Security Perimeter wiring external to a Physical Security Perimeter must be protected within a six-wall boundary. The team revised the interpretation based on stakeholder comments submitted during the initial ballot for the first draft of the interpretation.

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2008-10_CIP-006_Interpretation_Progress.html

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

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

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

Ballot Results	
Ballot Name:	Project 2008-10 Interpretation - Progress Energy - CIP-006-1 Revised_in
Ballot Period:	9/30/2009 - 10/12/2009
Ballot Type:	Initial
Total # Votes:	199
Total Ballot Pool:	249
Quorum:	**79.92 % The Quorum has been reached**
Weighted Segment Vote:	74.47 %
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.	70	1	39	0.75	13	0.25	1	17
2 - Segment 2.	11	0.8	5	0.5	3	0.3	1	2
3 - Segment 3.	57	1	35	0.778	10	0.222	3	9
4 - Segment 4.	10	0.9	6	0.6	3	0.3	1	0
5 - Segment 5.	46	1	25	0.735	9	0.265	2	10
6 - Segment 6.	30	1	17	0.773	5	0.227	3	5
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	9	0.6	3	0.3	3	0.3	0	3
9 - Segment 9.	8	0.3	3	0.3	0	0	2	3
10 - Segment 10.	8	0.7	7	0.7	0	0	0	1
Totals	**249**	**7.3**	**140**	**5.436**	**46**	**1.864**	**13**	**50**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips		
1	Ameren Services	Kirit S. Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Jason Shaver	Negative	View
1	Avista Corp.	Scott Kinney		
1	Baltimore Gas & Electric Company	John J. Moraski	Affirmative	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	

1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy	Paul Rocha	Negative	View
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	E.ON U.S. LLC	Larry Monday		
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Negative	View
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg		
1	ITC Transmission	Elizabeth Howell	Negative	View
1	JEA	Ted E Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon		
1	Kissimmee Utility Authority	Joe B Watson		
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	Rodney Hawkins	Affirmative	
1	Long Island Power Authority	Jonathan Appelbaum	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	National Grid	Manuel Couto		
1	New York Power Authority	Ralph Rufrano		
1	New York State Electric & Gas Corp.	Henry G. Masti		
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura		
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Oncor Electric Delivery	Charles W. Jenkins		
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	PacifiCorp	Mark Sampson		
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	View
1	Puget Sound Energy, Inc.	Catherine Koch	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Abstain	
1	SaskPower	Wayne Guttormson		
1	SCE&G	Henry Delk, Jr.	Negative	View
1	Seattle City Light	Pawel Krupa	Affirmative	
1	South Texas Electric Cooperative	Richard McLeon	Negative	
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	Southwestern Power Administration	Gary W Cox	Affirmative	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	Westar Energy	Allen Klassen	Negative	View
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Jason L. Murray	Negative	View
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Abstain	

2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Negative	View
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Jason L Marshall	Negative	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Affirmative	
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Negative	
3	American Electric Power	Raj Rana	Negative	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	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		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Farmington	Linda R. Jacobson	Abstain	
3	City Public Service of San Antonio	Edwin Les Barrow		
3	Commonwealth Edison Co.	Stephen Lesniak	Negative	
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		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Negative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Negative	View
3	Duke Energy Carolina	Henry Ernst-Jr		
3	Entergy Services, Inc.	Matt Wolf	Abstain	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	R Scott S. Barfield-McGinnis	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone		
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory David Woessner		
3	Lakeland Electric	Mace Hunter	Affirmative	
3	Lincoln Electric System	Bruce Merrill	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C Parent	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	Muscatine Power & Water	John Bos	Affirmative	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	John J. McCawley	Negative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	Zack Dusenbury	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Negative	View
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	Consumers Energy	David Frank Ronk	Affirmative	

4	Detroit Edison Company	Daniel Herring	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Northern California Power Agency	Fred E. Young	Abstain	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	Amerenue	Sam Dwyer	Negative	
5	Avista Corp.	Edward F. Groce	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Chelan County Public Utility District #1	John Yale		
5	City of Tallahassee	Alan Gale	Negative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consolidated Edison Co. of New York	Edwin E Thompson		
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Edison Mission Energy	Ellen Oswald		
5	Entergy Corporation	Stanley M Jaskot		
5	Exelon Nuclear	Michael Korchynsky	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	JEA	Donald Gilbert		
5	Kansas City Power & Light Co.	Scott Heidtbrink		
5	Lakeland Electric	Thomas J Trickey	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin		
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	Michigan Public Power Agency	James R. Nickel		
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Negative	
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Orlando Utilities Commission	Richard Kinas		
5	PacifiCorp Energy	David Godfrey	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Negative	View
5	RRI Energy	Thomas J. Bradish	Affirmative	
5	Sacramento Municipal Utility District	Bethany Wright	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	South California Edison Company	Ahmad Sanati		
5	Southeastern Power Administration	Douglas Spencer	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Abstain	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	View
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Eugene Water & Electric Board	Daniel Mark Bedbury	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Thomas Saitta		

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

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 — Interpretation - CIP-006 - Cyber Security — Physical Security of Cyber Security Assets (Project 2008-10)
Date of Initial Ballot: September 30, 2009 – October 12, 2009

Summary Consideration:

The interpretation drafting team thanks all who commented during the last posting of the revised interpretation for their interest and feedback. Commenters from the last posting of the revised interpretation provided constructive comments and concerns. The interpretation drafting team identified two general themes in the comments:

1. **Disagreement concerning whether wiring is a "Cyber Asset." Several commenters expressed concern that interpreting wiring within the definition of "Cyber Asset" expanded the requirements of the standard; and**
2. **That CIP-006-1, requirement R1.1 does not specifically discuss particular options that may be used as alternatives to a completely enclosed ("six-wall" border) and should not be addressed by this interpretation.**

In response to the comments received and reflective of the team's revisions to the interpretation, the interpretation drafting team responded as follows:

The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.

The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Voter	Entity	Segment	Vote	Comment
Edward P. Cox	AEP Marketing	6	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss

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

Voter	Entity	Segment	Vote	Comment
				wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Brock Ondayko	AEP Service Corp.	5	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Jason L. Murray	Alberta Electric System Operator	2	Negative	The AESO agrees that use of encryption and other logical access control methods may be sufficient in some cases, however that is not what the standard calls for. Logical access controls cannot provide physical protection, and the standard clearly calls for physical protection. Thus, this interpretation would have the effect of changing the standard. Standards are not to be changed through an interpretation. If the standard needs to be changed, then the AESO recommends that a drafting team be assembled to propose changes to the standard requirements.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Kenneth Goldsmith	Alliant Energy Corp. Services, Inc.	4	Negative	Wiring itself does not possess programmable intelligence, is not a cyber asset, and should not require the protection as detailed in CIP-006-1, R1. This level of protection will require entities to make considerable investments into atypical cable protection methods without a correpsonding gain in protection of the cyber assets within the ESP or the reliability of the Bulk Electric System.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				

Voter	Entity	Segment	Vote	Comment
Kirit S. Shah	Ameren Services	1	Negative	Requirement R1.1 does not specifically discuss wiring. However, the interpretation results in expanding this requirement.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				
Paul B. Johnson	American Electric Power	1	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Raj Rana	American Electric Power	3	Negative	n reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), AEP has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Jason Shaver	American Transmission Company, LLC	1	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), ATC has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Neither Requirement R1.1 (CIP-006-1) nor Requirement 3 (CIP-002-1) specifically discuss or identify wiring as a cyber asset which would need protection within a six wall barrier.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Paul Rocha	CenterPoint Energy	1	Negative	Upon further review of the interpretation provided for CIP_006-1 - R1.1, CenterPoint Energy agrees with the concerns of American Electric Power (AEP). The first part of R1.1 requires that "all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. " Therefore, it is our conclusion that the interpretation includes reference to a condition that should not occur if the entity is to be in compliance with CIP_006-1 - R1.1. Specifically, the statement pertaining to "wiring within the Electronic Security Perimeter that is external to a Physical Security Perimeter,..." should not occur (according to the requirements of R.1.1) and adds a level of complexity to what components/assets are covered and what is expected for compliance.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				
Daniel Herring	Detroit Edison Company	4	Negative	Detroit Edison's opinion is this interpretation is unnecessary and that protecting cabling between physical security perimeters fully contained within an otherwise adequately secured facility is that the cable is sufficiently protected following guidance provided by NIST for use in our nuclear plants.
Response: The IDT thanks you for your comment. While the team believes that this comment suggests a good practice, it believes that the comment is beyond the scope of the interpretation.				
Jalal (John) Babik	Dominion Resources, Inc.	3	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by "Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				

Voter	Entity	Segment	Vote	Comment
Mike Garton	Dominion Resources, Inc.	5	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by 'Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Louis S Slade	Dominion Resources, Inc.	6	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by "Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
William L. Thompson	Dominion Virginia Power	1	Negative	Dominion cannot approve this interpretation without fully understanding what is meant by "Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Douglas E. Hils	Duke Energy Carolina	1	Negative	Thank you for the opportunity to vote on this interpretation. We think that the interpretation is unclear and believe that this issue is best addressed in a comprehensive manner in a revision to the CIP standards.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Walter Yeager	Duke Energy Carolina	6	Negative	Thank you for the opportunity to vote on this interpretation. We think that the interpretation is unclear and believe that this issue is best addressed in a comprehensive manner in a revision to the CIP standards."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is				

Voter	Entity	Segment	Vote	Comment
relevant to the “alternative measures” question that is beyond the scope of this interpretation. The definition of “Cyber Asset” in the *NERC Glossary of Terms Used in Reliability Standards* includes “communication networks,” but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of “Cyber Asset,” Requirement R1 of CIP-006-1 does not apply to wiring.				
Edward C Stein	Edward C Stein	8	Negative	So you have a system where you can detect when someone has gained "unauthorized access" and you discover that someone has gained unauthorized access, does this mean that you have violated some Standard somewhere. In today's world where the use of the internet is required to exchange market and transmission data to RTOs, I believe that it is impossible to protect yourself from a hacker. The interpretation is politically correct but is does not prevent hacking.
Response: The drafting team thanks you for your comment. While the team appreciates your concern, it believes that this issue is beyond the scope of the interpretation.				
Kent Saathoff	Electric Reliability Council of Texas, Inc.	10	Affirmative	For clarity, we suggest that NERC add a comment in guidelines or FAQs to reflect that steel conduits are acceptable as a 6-wall enclosure for wiring.
Response: The drafting team thanks you for your comment. While the team appreciates your concern, it believes that this issue is beyond the scope of the interpretation.				
John J. Blazekovich	Exelon Energy	1	Negative	Exelon believes that this interpretation, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Requirement R1.1 does not specifically discuss wiring, nor does the requirement suggest options that can be used as alternatives to a completely enclosed ("six-wall") border. It is also not fully responsive to the interpretation request by limiting the response just to wiring.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the “alternative measures” question that is beyond the scope of this interpretation.				
Kim Warren	Independent Electricity System Operator	2	Negative	We reiterate our previous comment that although directionally the IESO is in favour of the intent of the interpretation, we believe the current interpretation wording may effectively modify the intention of the standard, which is inconsistent with NERC Reliability Standards Development Procedure. Whereas the standard clearly requires physical access control, the interpretation effectively relaxes and hence alters this requirement by permitting logical measures to control physical access. Although we believe the standard should be revised to allow alternative protective

Voter	Entity	Segment	Vote	Comment
				measures, that is not the issue being balloted. We believe revisions to CIP-006-1, Requirement R1.1 should be made in the future to specifically cater for logical measures to control physical access to the Critical Cyber Assets.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Elizabeth Howell	ITC Transmission	1	Negative	In reviewing the response that the SDT has provided to the Progress Energy Interpretation addressing Requirement R1.1 (specifically addressing security perimeter wiring), ITC has determined that the interpretation process, albeit inadvertently, resulted in expanding the requirements of the standard rather than interpreting the existing requirement. Neither Requirement R1.1 (CIP-006-1) nor Requirement 3 (CIP-002-1) specifically discuss or identify wiring as a cyber asset which would need protection within a six wall barrier.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Jason L Marshall	Midwest ISO, Inc.	2	Negative	The FAQ developed along with the original CIP standards specifically state that the standards are not intended to address the wires between facilities. While we agree that the suggested interpretation is a good idea for a future improvement to the standard, the interpretation process is intended to clarify what the standard says as originally drafted, not what we would like the standard to say. In the response to comments from the initial ballot, the drafting team pointed out that the FAQ is a reference document and not enforceable. While we agree this is true, it does point out what the intent of the drafting team was when writing the requirements and is thus critical to interpreting the CIP standards. Q11 in the FAQ is clear that the drafting team did not intend to include wiring. The drafting team stated that the requirement only applies to assets that are not owned by the Responsible Entity and that the Q11 in the FAQ only addressed non-owned assets. First, we assume that the drafting team is referring to leasing by thae statement "assets that are not owned" even though leasing is one form of ownership. Second, leasing of communications cirucits is only one example given in the answer to Q11 in the FAQ. Thus, we can't conclude that Q11 does not apply to all communication circuits. If

Voter	Entity	Segment	Vote	Comment
				the drafting team wants to apply the standard to the wiring in the request for interpretation, they need to submit a SAR to modify the standard.
Response: Thank you for your comment. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring. The drafting team has revised the interpretation.				
James D. Hebson	PSEG Energy Resources & Trade LLC	6	Negative	Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions on the subject. While the RFI response drating team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSEG agrees with CAL ISO's position that this interpretation should not be "....what should have been done," Southern Company's position the "....it actually reresents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice....," ISO New England's position that "....the interpretation adds requirements that are not already part of the Standard...." and PJM's position that: "....the interpretation adds requirements that are not already part of the Standard. EIP-006 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done." The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communication links between discrete perimeters, the interpretation moves into an area which the standard intentionally does no address." PSEG believes that the only appropriate was to reach agreement on Progress Energy's question is to submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum,an appropriate implementation schedule must also be issued."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Thomas Piascik	PSEG Power LLC	5	Negative	Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions for the subject. While the RFI response drafting team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSEG agrees with CAL ISO's position that this interpretation should not be "...what should have been done.", Southern Company's

Voter	Entity	Segment	Vote	Comment
				position that "...it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice...", ISO New England's position that "...the interpretation adds requirements that are not already part of the Standard..." and PJM's position that: "...the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address." PSEG believes that the only appropriate way to have agreement of Progress Energy's question is submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum, an appropriate implementation schedule must also be issued
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Kenneth D. Brown	Public Service Electric and Gas Co.	1	Negative	Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions for the subject. While the RFI response drafting team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSE&G agrees with CAL ISO's position that this interpretation should not be "...what should have been done.", Southern Company's position that "...it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice...", ISO New England's position that "...the interpretation adds requirements that are not already part of the Standard..." and PJM's position that "...the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address." PSE&G

Voter	Entity	Segment	Vote	Comment
				believes that the only appropriate way to have agreement of Progress Energy's question is submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum, an appropriate implementation schedule must also be issued.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Jeffrey Mueller	Public Service Electric and Gas Co.	3	Negative	"Comments from the last ballot of this interpretation clearly show a strongly diverse set of opinions for the subject. While the RFI response drafting team has done a diligent job of responding to those comments, it is clear that there will still be a strong divide on the issue. PSEG agrees with CAL ISO's position that this interpretation should not be "...what should have been done.", Southern Company's position that "...it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice...", ISO New England's position that "...the interpretation adds requirements that are not already part of the Standard..." and PJM's position that: "...the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address." PSEG believes that the only appropriate way to have agreement of Progress Energy's question is submit a SAR to address the issue via the standards approval process. If the team is unwilling to have the question settled by the SAR process, then, at a minimum, an appropriate implementation schedule must also be issued."
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not				

Voter	Entity	Segment	Vote	Comment
explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
Kyle M. Hussey	Public Utility District No. 2 of Grant County	1	Affirmative	I agree with this interpretation. This clarifies that wiring can not only be secured through physical means but also logical.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, approved appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation.				
Henry Delk, Jr.	SCE&G	1	Negative	SCE&G does not think the interpetation adds enough clarity. The issue should be addressed during development of the next set of NERC CIP Standards.
Response: Thank you for the comment. The Interpretation Drafting Team has revised the interpretation so that it limits itself to the specific question about wiring, and other issues raised regarding CIP-006-1 will be addressed in future versions.				
Hubert C. Young	South Carolina Electric & Gas Co.	3	Negative	SCE&G does not think the interpretation adds enough clarity. The issue should be addressed during development of the next set of NERC CIP standards.
Response: Thank you for the comment. The Interpretation Drafting Team has revised the interpretation so that it limits itself to the specific question about wiring, and other issues raised regarding CIP-006-1 will be addressed in future versions.				
Martin Bauer	U.S. Bureau of Reclamation	5	Affirmative	While Reclamation agrees with the interpretation, it is contingent on the basis that no TFE is required when Alternative Measures are deployed.
Response: Thank you for the comment. The Interpretation Drafting Team has revised the interpretation so that consideration of alternative measures and whether a TFE is required are beyond the scope of this Request for Interpretation.				
Allen Klassen	Westar Energy	1	Negative	Do not agree with wire as a cyber asset
Response: Thank you for your comment. The drafting team agrees and has revised the interpretation.				

Voter	Entity	Segment	Vote	Comment
Linda Horn	Wisconsin Electric Power Co.	5	Negative	Wisconsin Electric is concerned with the use of the term "effective security". This does not identify what type of physical protection is equivalent to six wall borders. Does cabling protected by metallic conduit constitute effective security? Communication networks utilizing fiber optic cabling is very difficult to splice in a tap allowing unapproved logical access. Does fiber optic cable require the same protective measures as copper? There are still questions or clarification required.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				
James R. Keller	Wisconsin Electric Power Marketing	3	Negative	Wisconsin Electric is concerned with the use of the term "effective security". This does not identify what type of physical protection is equivalent to six wall borders. Does cabling protected by metallic conduit constitute effective security? Communication networks utilizing fiber optic cabling is very difficult to splice in a tap allowing unapproved logical access. Does fiber optic cable require the same protective measures as copper? There are still questions or clarification required.
Response: Thank you for the comment. The drafting team has determined that the interpretation must be limited to the question asked: whether CIP-006-1 R1 applies to the aspects of the wiring that comprises the ESP. The drafting team has revised the interpretation to be limited accordingly. The team furthermore acknowledges and notes that a different interpretation, appended to CIP-006-3c as appendix 3, is relevant to the "alternative measures" question that is beyond the scope of this interpretation. The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definiton of "Cyber Asset," Requirement R1 of CIP-006-1 does not apply to wiring.				

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets
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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."
The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 3. The interpretation in CIP-006-3c, appendix 3, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets
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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the ~~Cyber Security Order 706 SAR drafting team~~CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:

~~The definition of Cyber Asset in the *NERC Glossary of Terms Used in Reliability Standards* includes communication networks. Physical media (wiring) is a component of a communication network within an Electronic Security Perimeter, but the wiring itself is not a separate Cyber Asset.~~

~~The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the Electronic Security Perimeter. Since the connective wiring is inside the Electronic Security Perimeter, Requirement R1.1 of CIP-006-1 applies.~~

~~CIP-006-1 R1.1 also provides: "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." For wiring within the Electronic Security Perimeter that is external to a Physical Security Perimeter, the alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to data encryption, and/or circuit monitoring to detect unauthorized access or physical tampering.~~

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."
The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g, "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 3. The interpretation in CIP-006-3c, appendix 3, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

Unofficial Comment Form for Interpretation of CIP-006-x for Progress Energy (Project 2008-10)

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the interpretation of CIP-006-x for Progress Energy (Project 2008-10). The electronic comment form must be completed by **November 21, 2011.**

Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or by telephone at 404-446-9691.

Background Information

The last successive ballot to this interpretation closed on October 12, 2009. Since that date, a project team from the CIP Interpretation Drafting Team reviewed and responded to the comments received from the last successive ballot and made revisions to the interpretation. The project team revised the interpretation pursuant to NERC Guidelines for Interpretation Drafting Teams (available here).

The interpretation drafting team determined that the interpretation must limit itself to the question asked: whether CIP-006-1, Requirement R1.1, applies to the aspects of wiring that comprises the ESP. The interpretation drafting team revised the interpretation from the last successive ballot accordingly.

The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but the interpretation drafting team determined that it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," the interpretation drafting team interpreted that Requirement R1.1 of CIP-006-1 does not apply to wiring.

The team furthermore acknowledges and notes in its revised interpretation that a different interpretation, appended to CIP-006-3c as appendix 3, applies to the "alternative measures" question "where a completely enclosed ('six-wall') border cannot be established" for "Cyber Assets within an Electronic Security Perimeter." The interpretation drafting team has determined that such analysis is beyond the scope of this interpretation. CIP-006-1 R1.1 applies to "Cyber Assets" and this interpretation is limited to whether wiring is a "Cyber Asset." A secondary analysis of "acceptable alternative measures where a completely enclosed ('six-wall') border cannot be established" does not apply.

You do not have to answer all questions. Enter All Comments in Simple Text Format.

Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.

Please review the request for an interpretation, the associated standard, and the draft interpretation and then answer the following questions.

1. The NERC Board of Trustees indicated that the interpretation process **should not** be used to address requests for a decision on **"how"** a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement?

   ☐ The request is asking for clarity on the **meaning** of a requirement.

☐ The request is asking for clarity on the **application** of a requirement.

Comments:

2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it 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. Do you believe this interpretation expands the reach of the standard?

   ☐ The interpretation **expands** the reach of the standard.

   ☐ The interpretation **does not expand** the reach of the standard.

   Comments:

3. Do you agree with this interpretation? If not, why not.

   ☐ Yes

   ☐ No

   Comments:

4. Are there any other comments you would like to add that haven't been covered in the previous questions, please add them here.

   Comments:

A. Introduction

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

2. Number: CIP-006-3c

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

4. Applicability:

4.1. Within the text of Standard CIP-006-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-3:

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

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

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

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

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

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

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
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.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	
3	12/16/09	Approved by NERC Board of Trustees	Update
1a	Board approved 02/12/ 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 (Appendix 1)	Interpretation (Project 2007-27)
1b/2b	Board approved 08/05/2009	Interpretation of R4 (Appendix 2)	Interpretation (Project 2008-15)
3c	Board approved 02/16/2010	Interpretation of R1 and R1.1 (Appendix 3)	Interpretation (Project 2009-13)

Appendix 1

Interpretation of Requirement R1.1.

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

Interpretation:

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

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

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

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

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

1.4. Additional Compliance Information

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

Appendix 2

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

Request:

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

Interpretation:

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

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

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

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

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

Appendix 3

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-10 Interpretation of CIP-006-x R1 for Progress Energy
Ballot Pool Forming October 12 – November 10, 2011
Formal Comment Period October 12 – November 21, 2011
Initial Ballot Window Open November 11 – 21, 2011

Project Webpage

An interpretation of CIP-006-x — Physical Security of Critical Cyber Assets has been posted for a formal comment period through 8 p.m. Eastern on Thursday, November 21, 2011. A new ballot pool is being formed and is open through 8 a.m. Eastern on Thursday, November 10th (note that ballot pools close at 8:00 *in the morning*, while comment periods and ballots close at 8:00 *in the evening*). An initial ballot of the interpretation will take place from Friday, November 11th through Monday, November 21st.

Instructions for Joining the Ballot Pool for Project 2008-10

Registered Ballot Body members may join the ballot pool to be eligible to vote in the upcoming ballot at the following page: Join

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-2008-10_CIP-006-1_SB_in@nerc.com

Instructions for Commenting

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

An initial ballot of the interpretation will begin on Friday, November 11th and will end at 8 p.m. Eastern on Monday, November 21, 2011.

Background

On April 2, 2008, clarification was requested by Progress Energy on CIP-006-1, specifically on whether Electronic Security Perimeter wiring external to a Physical Security Perimeter must be protected within a six-wall boundary.

Initial ballots ended on August 16, 2008, and October 12, 2009. In November 2009, the NERC Board of Trustees issued guidance concerning interpretations, and development of more formal process for addressing interpretations consistent with BOT guidance, as well as the overall workload d priorities of the Project 2008-06 CIP standards drafting team, resulted in a delay in further processing.

In June 2011, the Standards Committee established and appointed members for a standing CIP Interpretation Drafting Team to process the CIP-related interpretations that remain outstanding, including Project 2008-10. A new project team was formed for this interpretation from the CIP Interpretation Drafting Team. In developing the revised interpretation for this successive ballot, the team considered and discussed FERC Order No. 706 and subsequent versions of the CIP standards. In addition, since the previous versions of this interpretation were posted, the Standards Committee has published Guidelines for Interpretation Drafting Teams that were applied by the CIP Interpretation Drafting team.

Additional information on Project 2008-10 is available on the project webpage. Additional information on the activities of the CIP Interpretation Drafting Team is available on the team's webpage.

Standards Process

The Standard Processes Manual 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 Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-10 Interpretation of CIP-006-x R1 for Progress Energy

Successive Ballot Results

Now Available

A successive ballot of an interpretation of CIP-006-x — Physical Security of Critical Cyber Assets for Progress Energy concluded on November 21 2011. Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results.

Quorum: 83.53%

Approval: 95.99%

Next Steps

The drafting team will consider all comments received and determine whether to make additional changes to the interpretation. If the drafting team decides to make additional changes to the interpretation to address stakeholder feedback from the formal comment period and ballot, the team will post the revised interpretation, along with its consideration of comments, for a parallel comment period and successive ballot. If the drafting team decides that no substantive changes are required to address stakeholder feedback, the team will post the interpretation and consideration of comments for a recirculation ballot.

Background

On April 2, 2008, clarification was requested by Progress Energy on CIP-006-1, specifically on whether Electronic Security Perimeter wiring external to a Physical Security Perimeter must be protected within a six-wall boundary.

Initial ballots ended on August 16, 2008, and October 12, 2009. In November 2009, the NERC Board of Trustees issued guidance concerning interpretations, and development of more formal process for addressing interpretations consistent with BOT guidance, as well as the overall workload d priorities of the Project 2008-06 CIP standards drafting team, resulted in a delay in further processing.

In June 2011, the Standards Committee established and appointed members for a standing CIP Interpretation Drafting Team to process the CIP-related interpretations that remain outstanding, including Project 2008-10. A new project team was formed for this interpretation from the CIP Interpretation Drafting Team. In developing the revised interpretation for this successive ballot, the team considered and discussed FERC Order No. 706 and subsequent versions of the CIP standards. In addition, since the previous versions of this interpretation were posted, the Standards Committee has

published Guidelines for Interpretation Drafting Teams that were applied by the CIP Interpretation Drafting team.

Additional information on Project 2008-10 is available on the project webpage. Additional information on the activities of the CIP Interpretation Drafting Team is available on the team's webpage.

Standards Development Process

The Standard Processes Manual 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 Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2008-10 Interpretation CIP-006-1 Progress Energy Successive Ballot_in
Ballot Period:	11/11/2011 - 11/21/2011
Ballot Type:	Initial
Total # Votes:	279
Total Ballot Pool:	334
Quorum:	**83.53 % The Quorum has been reached**
Weighted Segment Vote:	95.99 %
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.	88	1	63	0.94	4	0.06	8	13
2 - Segment 2.	10	0.5	5	0.5	0	0	2	3
3 - Segment 3.	78	1	57	1	0	0	9	12
4 - Segment 4.	25	1	16	1	0	0	4	5
5 - Segment 5.	70	1	46	0.979	1	0.021	9	14
6 - Segment 6.	46	1	31	0.912	3	0.088	6	6
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.6	6	0.6	0	0	0	2
9 - Segment 9.	1	0.1	1	0.1	0	0	0	0
10 - Segment 10.	8	0.5	4	0.4	1	0.1	3	0
Totals	**334**	**6.7**	**229**	**6.431**	**9**	**0.269**	**41**	**55**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	View
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil		
1	Gainesville Regional Utilities	Luther E. Fair	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Lee County Electric Cooperative	John W Delucca	Abstain	
1	Lincoln Electric System	Doug Bantam	Abstain	
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	View
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena		
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	View
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery		
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch		
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	View
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Affirmative	

1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Abstain	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Negative	View
1	Southern Company Services, Inc.	Robert Schaffeld	Affirmative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox		
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	View
3	Alabama Power Company	Richard J. Mandes	Affirmative	View
3	Ameren Services	Mark Peters	Affirmative	
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Affirmative	
3	Consumers Energy	Richard Blumenstock	Abstain	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Gulf Power Company	Paul C Caldwell	Affirmative	View
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	

3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	View
3	Mississippi Power	Jeff Franklin	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	View
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone		
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Oregon Trail Electric Cooperative	ned ratterman		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Abstain	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Abstain	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Affirmative	View
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	View
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Abstain	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	

5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl		
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Edison Mission Energy	Ellen Oswald	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Abstain	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Oklahoma Gas and Electric Co.	Kim Morphis		
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Mikhail Falkovich	Abstain	
5	Puget Sound Energy, Inc.	Tom Flynn	Abstain	
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson	Affirmative	
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Affirmative	View
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	

5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	RANDY A YOUNG	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Imperial Irrigation District	Cathy Bretz		
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	View
6	New York Power Authority	William Palazzo		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Negative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Abstain	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Abstain	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	View
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Affirmative	
8		Edward C Stein	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Abstain	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	

10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

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

Account Log-In/Register

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Interpretation of CIP-006-x for Progress Energy (Project 2008-10)

The CIP-006-x for Progress Energy Drafting Team thanks all commenters who submitted comments on the interpretation for CIP-006-x for Progress Energy (Project 2008-10). These standards were posted for a 45-day public comment period from October 12, 2011 through November 21, 2011. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 17 sets of comments, including comments from approximately 56 different people from approximately 31 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2008-10_CIP-006_Interpretation_Progress.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Perry		SPP	10
2.	Shon Austin		SPP	10
3.	Ron Ciesiel		SPP	10

2.	Group	Connie Lowe	Electric Market Policy, Information Technology Risk Management	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		RFC	1
2.	Sean Iseminger		SERC	5
3.	Mike Garton		NPCC	5
4.	Michael Gildea		MRO	5

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
5. Louis Slade		RFC 6										
6. Michael Crowley		SERC 3										
3. Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Brian Evans-Mongeon	Utility Services	NPCC	8
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Chantel Haswell	FPL Group, Inc.		5
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1
11.	Michael R. Lombardi	Northeast Utilities	NPCC	1
12.	Randy Macdonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1
16.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
18.	Saurabh Saksena	National Grid	NPCC	1
19.	Michael Schiavone	National Grid	NPCC	1
20.	Wayne Sipperly	New York Power Authority	NPCC	5
21.	Tina Teng	Independent Electricity System Operator	NPCC	2
22.	Donald Weaver	New Brunswick System Operator	NPCC	2
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1
24.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3

4. Group	Nick Wehner	ACES Power Marketing Standards Collaborators						X				

Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. James Jones		Arizona Electric Power Cooperative/Southwest Transmission Company	WECC 1, 4, 5										
5.	Group	Steve Diebold	Kansas City Power & Light	X		X		X	X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Michael Gammon	KCPL	SPP	1, 3, 5, 6									
2.	Scott Harris	KCPL	SPP	1, 3, 5, 6									
3.	Dean Larson	KCPL	SPP	1, 3, 5, 6									
4.	Bob Beachy	KCPL	SPP	1, 3, 5, 6									
5.	Brett Holland	KCPL	SPP	1, 3, 5, 6									
6.	Individual	Antonio Grayson	Southern Company	X		X		X	X				
7.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
8.	Individual	Michael Falvo	Independent Electricity System Operator		X								
9.	Individual	Michael R. Lombardi	Northeast Utilities	X		X		X					
10.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
11.	Individual	Thad Ness	American Electric Power	X		X		X	X				
12.	Individual	Anthony Jablonski	ReliabilityFirst										X
13.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									
14.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
15.	Individual	Chris Higgins / Forrest Krigbaum & BPA CIP Team	Bonneville Power Administration	X		X		X	X				
16.	Individual	Rebecca Moore Darrah	MISO		X								
17.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				

1. **The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement?**

Summary Consideration:

Many commenters noted the request for interpretation is asking for clarity on the application of a requirement, while others noted the request for interpretation is asking for clarity on the meaning of a requirement. In general, the Interpretation Drafting Team ("IDT") agrees the Request for Interpretation ("RFI") asks in part for clarity on the application of the requirement ("*Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP*"). The IDT notes, however, that whether the requirement applies requires clarity on the meaning of the requirement ("*It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary*"). The IDT interpreted that "wire" is not part of the definition of "Cyber Asset," and that CIP-006-3c, R1.1, only applies to Cyber Assets, which provides clarity on the meaning and the application of the requirement.

Organization	Yes or No	Question 1 Comment
Kansas City Power & Light	The request is asking for clarity on the application of a requirement.	In this instance the request is asking for clarity in the application of the requirement, however, the interpretation response involved both the meaning of requirement CIP-002-1, R3 and the application of that meaning with CIP-006-1, R1.1.
Response: Thank you for your response. The IDT agrees the RFI appears to ask, in part, for clarity on the application of the requirement to a particular circumstance; however, the RFI also asks for clarity on the meaning of the requirement.		
ReliabilityFirst	The request is asking for clarity on the application	The last sentence of the Request for Interpretation reads (emphasis added): Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP. The meaning of the requirement appears to be reasonably clear. Progress

Organization	Yes or No	Question 1 Comment
	of a requirement.	Energy is requesting a determination of how to apply the requirement to a specific situation.
Response: Thank you for your response; the IDT agrees. The IDT agrees the RFI appears to ask, in part, for clarity on the application of the requirement to a particular circumstance; however, the RFI also asks for clarity on the meaning of the requirement.		
Southern Company	The request is asking for clarity on the application of a requirement.	The request specifically asks about the applicability of wiring.
Response: Thank you for your response; the IDT agrees. The IDT agrees the RFI appears to ask, in part, for clarity on the application of the requirement to a particular circumstance; however, the RFI also asks for clarity on the meaning of the requirement.		
Xcel Energy	The request is asking for clarity on the meaning of a requirement.	This request is defining what is considered a Critical Asset and not how to protect the Critical Assets.
Response: Thank you for the comment. The IDT agrees the interpretation provides clarity on the meaning of the requirement by clarifying that wire is not a Cyber Asset.		
Independent Electricity System Operator	The request is asking for clarity on the application	

Organization	Yes or No	Question 1 Comment
	of a requirement.	
Oncor Electric Delivery Company LLC	The request is asking for clarity on the application of a requirement.	
Southwest Power Pool Regional Entity	The request is asking for clarity on the meaning of a requirement.	
Electric Market Policy, Information Technology Risk Management	The request is asking for clarity on the meaning of a requirement.	
Northeast Power Coordinating Council	The request is asking for clarity on the meaning of a requirement.	
ACES Power Marketing Standards Collaborators	The request is asking for clarity on the	

Organization	Yes or No	Question 1 Comment
	meaning of a requirement.	
Manitoba Hydro	The request is asking for clarity on the meaning of a requirement.	
Northeast Utilities	The request is asking for clarity on the meaning of a requirement.	
Duke Energy	The request is asking for clarity on the meaning of a requirement.	
American Electric Power	The request is asking for clarity on the meaning of a requirement.	
American Transsmission Company, LLC	The request is asking for clarity on the meaning of a	

Organization	Yes or No	Question 1 Comment
	requirement.	
Bonneville Power Administration		
MISO		

2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it 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. Do you believe this interpretation expands the reach of the standard?

Summary Consideration:

Most balloters agree the interpretation does not expand the reach of the standard. However, one commenter expressed concern that the interpretation restricts the reach of the standard. In general, the IDT does not share this view, and notes that it must follow the guidelines set forth in the Guidelines for Interpretation Drafting Teams (available at: http://www.nerc.com/files/Guidelines_for_Interpretation_Drafting_Teams_Approved_April_2011.pdf). The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard.

Organization	Yes or No	Question 2 Comment
ReliabilityFirst	The interpretation does not expand the reach of the standard.	However, this interpretation greatly restricts the reach of CIP-006-3c R1.
Response: Thank you for your comment. While the IDT appreciates this concern, it disagrees that the interpretation restricts the reach of the standard. Rather, the purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard.		
Xcel Energy	The interpretation does not expand the reach of the standard.	The interpretation provided defines more clearly what should be included in the scope of standard.

Organization	Yes or No	Question 2 Comment
Response: Thank you for the comment, The IDT appreciates that its analysis of the language provides clarity.		
Southwest Power Pool Regional Entity	The interpretation does not expand the reach of the standard.	
Electric Market Policy, Information Technology Risk Management	The interpretation does not expand the reach of the standard.	
Northeast Power Coordinating Council	The interpretation does not expand the reach of the standard.	
ACES Power Marketing Standards Collaborators	The interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 2 Comment
Kansas City Power & Light	The interpretation does not expand the reach of the standard.	
Southern Company	The interpretation does not expand the reach of the standard.	
Manitoba Hydro	The interpretation does not expand the reach of the standard.	
Independent Electricity System Operator	The interpretation does not expand the reach of the standard.	
Northeast Utilities	The interpretation	

Organization	Yes or No	Question 2 Comment
	does not expand the reach of the standard.	
Duke Energy	The interpretation does not expand the reach of the standard.	
American Electric Power	The interpretation does not expand the reach of the standard.	
Oncor Electric Delivery Company LLC	The interpretation does not expand the reach of the standard.	
American Transmission Company, LLC	The interpretation does not expand the reach of the	

Organization	Yes or No	Question 2 Comment
	standard.	
MISO	The interpretation does not expand the reach of the standard.	
Bonneville Power Administration		

3. Do you agree with this interpretation? If not, why not.

Summary Consideration:

By overwhelming majority, most balloters agreed with the IDT's interpretation. However, there were some important minority viewpoints that the team considered. Almost universally, the viewpoints and concerns raised by commenters who did not agree with the interpretation were previously evaluated and considered in some manner during the development of the interpretation. In the responses that follow, and summarized here, the IDT explains the team's conclusions in developing the interpretation and how the team considered the comments. The team appreciated all of the comments and thanks participants for their input.

First, some commenters expressed concern that this interpretation conflicts with the interpretation in Appendix 1 of CIP-006-3c (see clarifying discussion, below, regarding usage of "Appendix 1" v. "Appendix 3" in reference to the interpretation developed by Project 2009-13). The IDT disagrees that this interpretation conflicts with Appendix 1, because there may be other scenarios beyond wiring for which Appendix 1 applies. Appendix 1 and this interpretation address different questions. This interpretation addresses whether wire is a Cyber Asset and Appendix 1 addresses alternative measures to a "six-wall" border for Cyber Assets.

Another commenter was concerned the interpretation would change the way standards are read and weaken the standard, but the IDT notes in its response the distinction between lists separated by "but not limited to" and the definition of "Cyber Asset," which is the subject of this interpretation. Furthermore, the IDT respectfully disagrees the interpretation weakens the standard, because the purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard.

In response to a comment that wire is a transport medium necessitating classification as a Cyber Asset and that wiring is an essential component of a network, the IDT explains that it respectfully disagrees on the bases that a transport medium is not the same as a communication network (and therefore not a Cyber Asset to which the requirement applies) and that essentiality of a component is not the criteria for application of the requirement in question.

One commenter noted the interpretation incorrectly referenced Appendix 3 of CIP-006-3c, and that the correct reference should be Appendix 1. In its interpretation, the IDT referred to the interpretation developed by Project 2009-13. That interpretation is now posted on the NERC Web site as Appendix 1 of CIP-006-3c; however, the interpretation developed by Project 2009-13 was Appendix 3 in the version of CIP-006-3c that accompanied the information for this project's (Project 2008-10) formal comment and successive ballot period materials. The numbering of the appendices in CIP-006-3c changed in September, 2011 (but not the content). The IDT agrees with the commenter that the reference should be corrected to refer to the latest posted version of CIP-006-3c, which is Appendix 1. Additionally, the IDT believes that it is clear from the context of the interpretation and the comments received that any references to "Appendix 3," both by commenters and the previously-posted version of this interpretation (Project 2008-10), refer to

the interpretation developed by Project 2009-13. In response to the comment, the IDT has changed the reference in the interpretation, which does not affect the substance of the interpretation. For purposes of these responses to comments, the IDT construes references to Appendix 1 and to Appendix 3 as references to the interpretation developed by Project 2009-13. As such, it is using the corrected reference to Appendix 1 in its responses for consistency, even if the commenter references Appendix 3.

Organization	Yes or No	Question 3 Comment
ReliabilityFirst	No	1. This interpretation is in direct conflict with Appendix 3 of CIP-006-3c. If wiring is not considered part of a network, then Appendix 3 of CIP-006-3c is not needed.2. This interpretation changes the way standards are read, and will require every reliability standard to be reviewed and possibly re-written. For example, FAC-008-3 R2.4.1 gives the scope as including, but not limited to, six types of equipment. If this interpretation passes, then FAC-008-3 will be read prescriptively. Any device not specifically listed will be out of scope for the requirement.3. From a cyber security perspective, this interpretation fatally weakens the protections of CIP-006-3c and CIP-005-3a. Running network cable outside of a Physical Security Perimeter without some form of compensating measure is exposing the data from within an ESP to possible compromise and attack.

Response: Thank you for your comments. The IDT discussed and evaluated all of these concerns in its deliberations of developing the interpretation. The following explanations, which correspond with the numbering of your comments, discuss the IDT's consideration of your concerns:

1) **The IDT disagrees that this interpretation is in direct conflict with Appendix 1 of CIP-006-3c (See explanation of "Appendix 1" v. "Appendix 3" usage in the Summary Consideration to Question 3, above). There may be other scenarios beyond wiring for which Appendix 1 applies.**
2) **The IDT respectfully disagrees. In the example given of FAC-008-3, and in many other standards' requirements, the language includes the phrase, "but not limited to," which specifically precludes a prescriptive reading of the enumerated items. Furthermore, the IDT is not changing the scope of what is enumerated in determining what is a Cyber Asset; instead, it is clarifying that "wire" is not explicitly included within the meaning of "communication network," which is enumerated in the language of the definition of "Cyber Asset."**
3) **While the IDT appreciates this concern, it disagrees that the interpretation weakens the protections of CIP-006 and CIP-005**

Organization	Yes or No	Question 3 Comment
because it is not contrary to any requirement to protect data.		
Southwest Power Pool Regional Entity	No	SPP RE does not agree with this interpretation for two reasons. 1. The NERC Glossary defines a Cyber Asset as "Programmable electronic devices and communication networks including hardware, software, and data." The wire is the transport medium for the data, and data is a cyber asset. CIP-006-3 R1.1 requires data to be protected; to protect the data, the wire must also be protected. 2. Wiring can be viewed as an essential component of the hardware comprising a network, further supporting the need to protect the wiring.
Response: The IDT thanks you for your comments. The IDT considered and evaluated these concerns in its deliberations. The following explanations, which correspond with the numbering of your comments, discuss the IDT's consideration of your concerns: **1. The IDT determined that wire is an underlying component of a Cyber Asset, much like air is the transport medium in a wireless network. However, wire or air itself is not a "communication network" (and therefore not a Cyber Asset), which is not contrary to CIP-006-3c, R1.1's requirement to protect data.** **The IDT appreciates this concern, but notes that it is outside the scope of the language of the definition of "Cyber Asset," and CIP-006-3c, R1.1's application is limited to Cyber Assets. Power and facilities are also essential components, but whether they are essential is not the criteria for application of CIP-006-3c, R1.1, which is the subject of this interpretation. The purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard.**		
Kansas City Power & Light	No	The question raised by Progress Energy is not clear enough for an appropriate interpretive response. As a result, the interpretive response may be including assumptions that were not stated in the question posed by Progress Energy. At any rate, it is recommended that Progress Energy be afforded the opportunity to resubmit their question with additional information and circumstances regarding the communications mediums leaving the Physical Security Perimeter under consideration.

Organization	Yes or No	Question 3 Comment
Response: The IDT thanks you for your comment, but it disagrees that the request for interpretation is not clear enough for an interpretive response. The IDT believes it has provided clarity to the meaning of the requirement through its analysis.		
Southern Company	Yes	However, the interpretation incorrectly refers to Appendix 3 of CIP-006-3c. The language should be corrected to refer to Appendix 1 of CIP-006-3c.
Response: The IDT thanks you for this comment. In its reference to "Appendix 3," the IDT referred to the interpretation developed by Project 2009-13. That interpretation is now posted as Appendix 1 of CIP-006-3c; however, the interpretation developed by Project 2009-13 was labeled as Appendix 3 in the version of CIP-006-3c that accompanied the information for this project's (Project 2008-10) formal comment and successive ballot period materials on the Project 2008-10 project page. The numbering of the appendices in CIP-006-3c changed in September, 2011 (but not the content). The IDT agrees with the commenter that the reference should be corrected to refer to the latest posted version of CIP-006-3c, which is Appendix 1. Additionally, the IDT believes that it is clear from the context of the comments received that references to "Appendix 3," both by commenters and the previously-posted version of this interpretation (Project 2008-10), refer to the interpretation developed by Project 2009-13. In response, the IDT has changed the reference in the interpretation, which does not affect the substance of the interpretation.		
Electric Market Policy, Information Technology Risk Management	Yes	
Northeast Power Coordinating Council	Yes	
ACES Power Marketing Standards Collaborators	Yes	
Manitoba Hydro	Yes	
Independent Electricity	Yes	

Organization	Yes or No	Question 3 Comment
System Operator		
Northeast Utilities	Yes	
Duke Energy	Yes	
American Electric Power	Yes	
Oncor Electric Delivery Company LLC	Yes	
American Transsmission Company, LLC	Yes	
MISO	Yes	
Xcel Energy	Yes	
Bonneville Power Administration		

4. Are there any other comments you would like to add that haven't been covered in the previous questions, please add them here.

Summary Consideration:

Some commenters expressed concern about the distinction between Appendix 1 of CIP-006-3c and this interpretation (See explanation of "Appendix 1" v. "Appendix 3" usage in reference to Project 2009-13 in the Summary Consideration to Question 3, above). This interpretation is distinct because it only addresses whether wire is a "Cyber Asset." The IDT notes that, while Appendix 1 may have used "wire" as an example, Appendix 1 applies only upon a determination that something is a Cyber Asset. This interpretation clarifies that wiring is not a Cyber Asset.

One commenter thought the interpretation should have been an initial ballot, but the IDT notes that a successive ballot is appropriate under the current NERC Standard Processes Manual when making a substantive change to the previously-posted interpretation.

Organization	Yes or No	Question 4 Comment
Bonneville Power Administration		BPA thanks you for the opportunity to comment on Project 2008-10 Interpretation of CIP-006-1 R1 for Progress Energy. BPA has no comments or concerns at this time.
Response: Thank you for your participation		
MISO		In general, the Midwest Independent Transmission System Operator (the "MISO") supports the revised interpretation of CIP-006-1, Requirement R1.1 (the "2008-10 Interpretation") developed by the CIP Interpretation Drafting Team (the "IDT"). In particular, MISO agrees with the IDT that wiring does not meet the definition of "Cyber Asset" in the NERC Glossary of Terms Used in Reliability Standards and that Requirement R1.1 therefore does not apply to wiring. MISO is concerned, however, that there is an inconsistency between the 2008-10 Interpretation and the interpretation in CIP-006-3c, appendix 3 ("Appendix 3"). Appendix 3 states that "[f]or Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets [ ] Requirement R1.1 as not limited to measures that are 'physical in nature'" (emphasis added). This language implies that wiring is subject to Requirement R1.1. The 2008-10 Interpretation, however, states unambiguously that

Organization	Yes or No	Question 4 Comment
		wiring is not a Cyber Asset and is not subject to Requirement R1.1. The IDT is clearly aware of this inconsistency, as it included the following language in the interpretation:This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 3. The interpretation in CIP-006-3c, appendix 3c, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).This limitation of the 2008-10 Interpretation does not, however, resolve the identified inconsistency because Appendix 3 explicitly addresses wiring, which means it is not "distinct" from the 2008-10 Interpretation. Thus, while MISO supports the approval of the 2008-10 Interpretation, MISO also urges the IDT to amend Appendix 3 or otherwise clarify that Appendix 3 does not apply to wiring.
Response: Thank you for your comment. The IDT disagrees that this interpretation is in direct conflict with Appendix 1 of CIP-006-3c (See explanation of "Appendix 1" v. "Appendix 3" usage in reference to Project 2009-13 in the Summary Consideration of Question 3, above). There may be other scenarios beyond wiring for which Appendix 1 applies. The purpose of the interpretation is to consider the language as written, within the Guidelines for Interpretation Drafting Teams, and to provide clarity on the meaning of the standard. The IDT notes that, while Appendix 1 may have used "wire" as an example, Appendix 1 applies only upon a determination that something is a Cyber Asset. This interpretation clarifies that wiring is not a Cyber Asset.		
ReliabilityFirst		This ballot should not be a successive ballot, but rather an initial ballot, as the text of the interpretation has been completely changed.
Response: The IDT thanks you for your comment, but notes that a successive ballot was called for pursuant to the NERC Standards Processes Manual. While the text completely changed, it was a substantive change necessitating a successive ballot.		
Southwest Power Pool Regional Entity		We disagree with the assertion: "This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 3. The interpretation in CIP-006-3c, appendix 3, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter

Organization	Yes or No	Question 4 Comment
		(ESP)."The interpretation in CIP-006-3C, Appendix 3 is directly applicable to Interpretation of CIP-006-1 Cyber Security - Physical Security of Critical Cyber Assets for Progress Energy. The interpretation found in Appendix 3 does provide for alternative means other than physical protection for instances in which physical protection is not technically feasible. Implementation of those alternative means addresses instances in which data must traverse beyond a traditional "six-wall" boundary.
Response: The IDT thanks you for your comment. This interpretation is distinct because it only addresses whether wire is a "Cyber Asset." The IDT notes that, while Appendix 1 may have used "wire" as an example, Appendix 1 applies only upon a determination that something is a Cyber Asset. This interpretation clarifies that wiring is not a Cyber Asset. There may be other scenarios beyond wiring for which Appendix 1 applies.		
Southern Company		We would seek guidance or direction on how this interpretation applies to all versions of the approved standards. If this guidance is already available, please include a preamble providing how the interpretation will apply to all approved versions of the CIP-006 standard (i.e. CIP versions 1 through 4).
Response: The IDT thanks you for your question. An approved interpretation will be applied as equally relevant to all prior and subsequent versions of the standard to the extent the language of the relevant requirement language is the same in substance. The IDT anticipates that this interpretation, subject to industry, NERC Board of Trustees, and FERC approval, will be equally applicable to CIP-006, Versions 1 through Version 4 (The IDT notes that Version 4 remains pending as of this response, and its answer here assumes approval as filed by NERC to FERC).		
Electric Market Policy, Information Technology Risk Management		
ACES Power Marketing Standards Collaborators		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro		
Independent Electricity System Operator		
Northeast Utilities		
Duke Energy		
American Electric Power		
Oncor Electric Delivery Company LLC		
American Transsmission Company, LLC		
Xcel Energy		

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets
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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."
The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 1. The interpretation in CIP-006-3c, appendix 1, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets
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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

Interpretation of CIP-006-1 Requirement R1.1*: "…to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.*

Revised Response:

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."
The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g., "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix ~~3~~1. The interpretation in CIP-006-3c, appendix ~~3~~1, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

A. Introduction

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

2. Number: CIP-006-3c

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

4. Applicability:

4.1. Within the text of Standard CIP-006-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-3:

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

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

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

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

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

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

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -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.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24, 2011	Adopted by NERC Board of Trustees	
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	

Appendix 1

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

Appendix 2

Interpretation of Requirement R1.1.

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

Interpretation:

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

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

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

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

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

1.4. Additional Compliance Information

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

Appendix 3

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-10 Interpretation of CIP-006-x R1 for Progress Energy
Recirculation Ballot Window Open: December 9 - 19, 2011

Now Available

A recirculation ballot window is open for Project 2008-10 Interpretation of CIP-006-x R1 for Progress Energy from Friday, December 9, 2011 through 8 p.m. Eastern on Monday, December 19, 2011.

Since the initial ballot, the drafting team has considered all comments received during the formal comment period and successive ballot of the interpretation, and made no substantive changes to the interpretation. Only one change was made, to correct a reference to a prior interpretation of the same standard.

In its interpretation, the drafting team made a reference to a prior interpretation developed by Project 2009-13, which was Appendix 3 in the version of CIP-006-3c that accompanied the formal comment and successive ballot period materials. However, since that posting, the drafting team was made aware that the interpretation developed by Project 2009-13 is now posted as Appendix 1 of CIP-006-3c. The numbering of the appendices in CIP-006-3c changed in September 2011 (but not the content). The reference in this interpretation was updated to refer to the latest posted version of CIP-006-3c, which is Appendix 1.

Documents associated with this project, including clean and redline copies of the interpretation, the standard, and the drafting team's consideration of comments submitted during the parallel formal comment period and successive ballot that ended on November 21, 2011, have been posted on the project page.

Instructions for Balloting in the Recirculation Ballots

In a recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their prior votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's last vote cast in the successive ballot that ended on November 21, 2011 will be carried over.

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

Next Steps

If the interpretation achieves ballot pool approval, they will be presented to the Board of Trustees for adoption and subsequently filed with regulators for approval.

Background

On April 2, 2008, clarification was requested by Progress Energy on CIP-006-1, specifically on whether Electronic Security Perimeter wiring external to a Physical Security Perimeter must be protected within a six-wall boundary.

Initial ballots ended on August 16, 2008, and October 12, 2009. In November 2009, the NERC Board of Trustees issued guidance concerning interpretations, and development of more formal process for addressing interpretations consistent with BOT guidance, as well as the overall workload d priorities of the Project 2008-06 CIP standards drafting team, resulted in a delay in further processing.
In June 2011, the Standards Committee established and appointed members for a standing CIP Interpretation Drafting Team to process the CIP-related interpretations that remain outstanding, including Project 2008-10. A new project team was formed for this interpretation from the CIP Interpretation Drafting Team. In developing the revised interpretation for this successive ballot, the team considered and discussed FERC Order No. 706 and subsequent versions of the CIP standards. In addition, since the previous versions of this interpretation were posted, the Standards Committee has published Guidelines for Interpretation Drafting Teams that were applied by the CIP Interpretation Drafting team.

Additional information on Project 2008-10 is available on the project webpage. Additional information on the activities of the CIP Interpretation Drafting Team is available on the team's webpage.

Standards Development Process

The Standard Processes Manual 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 Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-10 Interpretation of CIP-006-x for Progress Energy

Recirculation Ballot Results

Now Available

A recirculation ballot of an interpretation of CIP-006-x Requirement R6 concluded on December 19, 2011. The interpretation was approved by the ballot pool. Voting statistics are listed below, and the Ballot Results webpage provides a link to the detailed initial ballot results.

Recirculation Ballot Results
Quorum: 88.02%
Approval: 96.04%

Next Steps
The interpretation will be presented to the NERC Board of Trustees for action, and if adopted, filed with regulatory authorities.

Background
On April 2, 2008, clarification was requested by Progress Energy on CIP-006-1, specifically on whether Electronic Security Perimeter wiring external to a Physical Security Perimeter must be protected within a six-wall boundary.

Initial ballots ended on August 16, 2008, and October 12, 2009. In November 2009, the NERC Board of Trustees issued guidance concerning interpretations, and development of more formal process for addressing interpretations consistent with BOT guidance, as well as the overall workload d priorities of the Project 2008-06 CIP standards drafting team, resulted in a delay in further processing.

In June 2011, the Standards Committee established and appointed members for a standing CIP Interpretation Drafting Team to process the CIP-related interpretations that remain outstanding, including Project 2008-10. A new project team was formed for this interpretation from the CIP Interpretation Drafting Team. In developing the revised interpretation for this successive ballot, the team considered and discussed FERC Order No. 706 and subsequent versions of the CIP standards. In addition, since the previous versions of this interpretation were posted, the Standards Committee has published Guidelines for Interpretation Drafting Teams that were applied by the CIP Interpretation Drafting team.

Additional information on Project 2008-10 is available on the project webpage. Additional information on the activities of the CIP Interpretation Drafting Team is available on the team's webpage.

Standards Development Process

The Standard Processes Manual 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 Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2008-10 Interpretation CIP-006-1 Progress Energy Successive Ballot_rc
Ballot Period:	12/9/2011 - 12/19/2011
Ballot Type:	recirculation
Total # Votes:	294
Total Ballot Pool:	334
Quorum:	**88.02 % The Quorum has been reached**
Weighted Segment Vote:	96.04 %
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.	88	1	67	0.931	5	0.069	8	8
2 - Segment 2.	10	0.6	6	0.6	0	0	2	2
3 - Segment 3.	78	1	61	1	0	0	7	10
4 - Segment 4.	25	1	16	1	0	0	5	4
5 - Segment 5.	70	1	49	1	0	0	10	11
6 - Segment 6.	46	1	33	0.892	4	0.108	5	4
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.7	7	0.7	0	0	0	1
9 - Segment 9.	1	0.1	1	0.1	0	0	0	0
10 - Segment 10.	8	0.6	5	0.5	1	0.1	2	0
Totals	**334**	**7**	**245**	**6.723**	**10**	**0.277**	**39**	**40**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	View
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil		
1	Gainesville Regional Utilities	Luther E. Fair	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Lee County Electric Cooperative	John W Delucca	Abstain	
1	Lincoln Electric System	Doug Bantam	Abstain	
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	View
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena		
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	View
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	View
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Affirmative	

1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Abstain	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Abstain	
1	South California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Affirmative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox		
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	View
3	Alabama Power Company	Richard J. Mandes	Affirmative	View
3	Ameren Services	Mark Peters	Affirmative	
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Affirmative	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Gulf Power Company	Paul C Caldwell	Affirmative	View
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	

3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	View
3	Mississippi Power	Jeff Franklin	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone		
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Oregon Trail Electric Cooperative	ned ratterman		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Abstain	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Abstain	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Affirmative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	View
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Abstain	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	

5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Abstain	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl		
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Edison Mission Energy	Ellen Oswald	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Abstain	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Oklahoma Gas and Electric Co.	Kim Morphis		
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Fossil LLC	Mikhail Falkovich	Abstain	
5	Puget Sound Energy, Inc.	Tom Flynn	Abstain	
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson	Affirmative	
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	View
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	

5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	RANDY A YOUNG	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Imperial Irrigation District	Cathy Bretz		
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	View
6	New York Power Authority	William Palazzo	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Abstain	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Abstain	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	View
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini	Affirmative	
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Abstain	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	

10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

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

Account Log-In/Register

Exhibit E

Roster of the interpretation drafting team for the Interpretation of Requirement R.1.1 of CIP-006-4

Name and Title	Company and Address	Contact Info	Bio
Tim Conway, Co-Chair Director, NERC Compliance and Operations Technology	NIPSCO 1500 165th ST Hammond, IN	(219) 853-4202 – Business tjconway@nisource.com	Mr. Conway is Director of NERC Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO). Formerly, he was an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He is the former Chair of the RFC CIPC and current Co-Chair of the NERC CIP Interpretation Drafting Team. Mr. Conway holds an MBA from the University of Notre Dame, a BS in Electrical Engineering Technology from Purdue University, and he has the obtained following professional certifications throughout his career: RHCT, SANS GCIH, CNE, Network +, CCNA, CISA, CRISC.
Scott Miller, Co-Chair Manager Corporate Affairs	MEAG Power 1407 Riveredge Parkway NW Atlanta, GA 30328 (678) 644-3524 - Business smiller@meagpower.org	(678) 644-3524 - Business smiller@meagpower.org	Mr. Miller actively works with American Public Power Association (APPA) and the Large Public Power Council (LPPC) Reliability Team to develop multi-company responses and positions on CIP standard developments as well as other NERC standards. He is an active member of the NERC Quality Review Team, and he has completed SOS NERC Training modules for relays, power plant operations, security, and other topics. Responsibilities include working on cyber issues that require the continual studying of cyber network and network security texts, and to monitor and review Congressional, FERC and NERC committee hearings, meetings and webinars. He has more than 30 years of electric and natural gas industry experience, which includes providing research, proposals, and testimony to FERC and the Illinois Commerce Commission as the primary liaison and witness on gas and electric rate making, engineering practices, and accounting/equipment life cycle studies. At MEAG Power, he provides 25 municipal electric distribution utilities with system planning and operational support. Mr. Miller has held various management and executive staff positions, and he is a USAF veteran and holds a BA and an MBA with an emphasis in numerical analysis. He is a member of the NERC CIP Interpretation Drafting Team.

Name and Title	Company and Address	Contact Info	Bio
Mark Engels Enterprise Technology Security & Compliance Director	Dominion 707 East Main Street Richmond, VA 23219	(804) 775-5263 – Business mark.engels@dom.com	Mark Engels is the Enterprise Technology Security and Compliance Director at Dominion and has been with the company 33 years. Mr. Engels is formerly a member of NERC's Cyber Security Standard Education Team (CSSET), which created the compliance audit presentation used at three NERC sponsored 1200 standard workshops and created the compliance audit presentation used at 10 NERC sponsored CIP-002-1 through CIP-009-1 standard workshops. Mr. Engels is currently a member of NERC's Critical Infrastructure Protection Committee (CIPC), chair of the NERC Control System Security Working Group (CSSWG), chair of the NERC Cyber Attack Task Force, and a member of the Southeastern Electric Reliability Corporation (SERC) CIPC leadership committee. He is a member of the NERC CIP Interpretation Drafting Team.
Jeffrey Fuller Senior Manager, Enterprise Security Services			Jeffrey Fuller is responsible for the management of the Enterprise Security department at his company, including cyber security, contract security, security incident response plans, risk assessments, and auditing activities. He has managed the Critical Infrastructure Protection (CIP) Program as well as industry SOX and PCI compliance requirements. Mr. Fuller is an active member of the NERC and RFC CIPC as well as an observer of the NERC Project 2008-06 SDT and other working groups. He brings a background that includes experience in IT, law enforcement, and compliance. He is a member of the NERC CIP Interpretation Drafting Team. Education: BS – Information Technology – WGU School of Police Staff and Command - NWU Certifications: Certified Information Systems Security Professional (CISSP) / Microsoft Certified Systems Engineer (MCSE) / Microsoft Certified Systems Administrator (MCSA) / Cisco Certified Network Associate (CCNA) / Microsoft Certified Desktop Support Technician (MCDST) / Microsoft Certified Trainer (MCT) / CompTIA Security+, Network+ and A+.

Name and Title	Company and Address	Contact Info	Bio
Trevor MacCrae Staff Compliance Analyst	Southern Company Transmission 600 N. 18th St., M/S 7S-8220 Birmingham, AL 35203	205-257-6210 – Business tmaccrae@southernco.com	As the senior EMS compliance analyst for Southern Company, Mr. MacCrae focuses on cybersecurity regulatory compliance for Transmission Energy Management Systems (SCADA) including strategy, process management, performance improvement, and compliance systems implementation. He is the Technical Feasibility Exception (TFE) program lead and a frequent contributor and team member participating in EMS programs related to audits, peer reviews, and industry groups. He has a Bachelor's Degree in Information Technology and an MBA with a concentration in Operations Management. He is a certified information systems security professional (CISSP) and recently passed the certified information security manager (CISM) examination. He serves as a Subject Matter Expert for the Electric Sector Cybersecurity Risk Management Maturity initiative, a U.S. Department of Energy program. He also serves as a member of the Industrial Control Systems Joint Working Group (ICSJWG) and is a member of the Roadmap to Secure Industrial Control Systems Subgroup. The DHS Control Systems Security Program (CSSP) established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing to reduce the risk to the nation's industrial control systems. He also serves as a member of the Utility Information Technology Benchmark and Best Practices (UNITE) NERC CIP team, which is a standing utility industry benchmarking team that shares benchmarking and best practices among its utility industry members. He is a member of the NERC CIP Interpretation Drafting Team.
Brian Newell Senior Instrumentation and Controls Engineer	American Electric Power 1 Riverside Plaza, 21st Floor Columbus, OH 43215	(614)716-2106 - Business benewell@aep.com	Brian Newell is a Senior Instrumentation and Controls Engineer with American Electric Power (AEP). Brian joined AEP in 2004. Previously, he was with ABB and Bailey Controls Company in engineering and technical support roles. Brian has over 14 years of experience with Distributed Control System (DCS) and Programmable Logic Controller (PLC) design, engineering, and testing. He has extensive experience in DCS, PLC, protective relay, data recorder, and Remote Terminal Unit (RTU) communications, networking, and security implementation from multiple vendor products. His current responsibilities include serving as a subject matter expert for the cyber security program implementation across the control, monitoring, and protection system equipment for AEP's Fossil and Hydro Generation fleet. He has also been an active observer of the NERC CIP Standards Drafting Team for over 2 years. Brian is a licensed Professional Engineer in Ohio. He is a member of the NERC CIP Interpretation Drafting Team.

Name and Title	Company and Address	Contact Info	Bio
Robert Ulmer CIP Compliance Consultant	American Transmission Company P.O. Box 47 Waukesha, WI 53188	(262) 506-6850 rulmer@atcllc.com	Robert Ulmer is responsible for American Transmission Company's (ATC) NERC Critical Infrastructure Protection (CIP) compliance program and he is a former CIP senior manager. He is also an alternate MRO member on the NERC CIPC. Mr. Ulmer joined ATC in 2001 as director of corporate services where he established ATC's information technology and security functions. In 2008, he was appointed project director for the construction of ATC's system control center and corporate headquarters in Waukesha, Wisconsin. Prior to joining ATC, Mr. Ulmer held a number of positions at We Energies and subsidiaries in nuclear power, finance, human resources, and co-generation projects in Latin America. He is a graduate of Carroll University and the University of Michigan Executive Program. He is a member of the NERC CIP Interpretation Drafting Team.