November 17, 2009

VIA ELECTRONIC FILING

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

Re: *North American Electric Reliability Corporation,*
Docket No. RM06-16-000

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits this petition in accordance with Section 215(d)(1) of the Federal Power Act ("FPA") and Part 39.5 of the Federal Energy Regulatory Commission's ("FERC") regulations seeking approval for interpretation of Requirement R2 in FERC-approved NERC Reliability Standard CIP-007-2 — Cyber Security — Systems Security Management.[1] The standard that includes the appended interpretation is designated as CIP-007-2a and is set forth in **Exhibit A** to this petition.

[1] At the time the request for interpretation was submitted in March 2009, Version 1 of CIP-007 was the only FERC-approved version in effect. The request was therefore processed referencing CIP-007-1. Since then, CIP-007 Version 2 has been submitted and approved by FERC in *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, Docket No. RD09-7-000 (September 30, 2009) ("September 30 CIP Version 2 Order"). CIP-007-2 takes effect on April 1, 2010. The changes to Requirement R2 in Version 2 relative to Version 1 of CIP-007 are not material to the substance of the interpretation request under consideration. In this regard, NERC will append the interpretation to Version 2 of the CIP-007 standard in lieu of Version 1.

The interpretation was approved by the NERC Board of Trustees on November 5, 2009. NERC requests this interpretation be made effective immediately upon approval by FERC.

NERC's petition consists of the following:

- This transmittal letter;
- A table of contents for the filing;
- A narrative description explaining how the interpretation meets the reliability goal of the standard involved;
- Interpretation of CIP-007-2, Requirement R2 submitted for approval (**Exhibit A**);
- Reliability Standard CIP-007-2a — Cyber Security — Systems Security Management that includes the appended interpretation (**Exhibit B**);
- The complete development record of the interpretation (**Exhibit C**); and
- The interpretation development team roster (**Exhibit D**).

Please contact the undersigned if you have any questions.

Respectfully submitted,

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

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**) Docket No. RM06-16-000)**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF AN INTERPRETATION TO RELIABILITY STANDARD CIP-007-2 — CYBER SECURITY — SYSTEMS SECURITY MANAGEMENT

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

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

November 17, 2009

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[2] hereby requests the Federal Energy Regulatory Commission ("FERC") to approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[3] and Section 39.5 of FERC's regulations, 18 C.F.R. § 39.5, an interpretation to a requirement of a FERC-approved NERC Reliability Standard: CIP-007-2[4] — Cyber Security — Systems Security Management, Requirement R2.

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-007-2 — Cyber Security — Systems Security Management, Requirement R2 on November 5, 2009. NERC requests that FERC approve this interpretation and make it effective immediately after approval in accordance with FERC's procedures. **Exhibit A** to this filing sets forth the interpretation. **Exhibit B** contains the affected Reliability Standard that includes the appended interpretation. **Exhibit C** contains the complete development record of the interpretation to CIP-007-2a, Requirement.R2. **Exhibit D** contains the interpretation development team roster.

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

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

[4] At the time the request for interpretation was submitted in March 2009, Version 1 of CIP-007 was the only FERC-approved version in effect. The request was therefore processed referencing CIP-007-1. Since then, CIP-007 Version 2 has been submitted and approved by FERC in *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, Docket No. RD09-7-000 (September 30, 2009) ("September 30 CIP Version 2 Order"). CIP-007-2 takes effect on April 1, 2010. The changes to Requirement R2 in Version 2 relative to Version 1 of CIP-007 are not material to the substance of the interpretation request under consideration. In this regard, NERC will append the interpretation to Version 2 of the CIP-007 standard in lieu of Version 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:

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

*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.

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

III. BACKGROUND

a. Regulatory Framework

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

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

operators of the bulk power system in the United States will be subject to FERC-approved Reliability Standards.

b. Basis for Approval of Proposed Interpretation

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

c. Reliability Standards Development Procedure and Interpretation

All persons who are directly or materially affected by the reliability of the North American bulk power system are permitted to request an interpretation of a Reliability Standard, as discussed in NERC's *Reliability Standards Development Procedure*, which is incorporated into the Rules of Procedure as Appendix 3A.[6] Upon request, NERC assembles a team with the relevant expertise to address the interpretation request and, within 45 days, present the interpretation for industry ballot. If approved by the ballot pool and the NERC Board of Trustees, the interpretation is appended to the Reliability Standard and filed for approval by FERC and applicable governmental authorities in Canada to be made effective when approved. When the affected Reliability Standard is next revised using the Reliability Standards Development Process, the interpretation will then be incorporated into the Reliability Standard.

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

The interpretation set out in **Exhibit A** has been developed and approved by industry stakeholders using NERC's *Reliability Standards Development Procedure.*[7] It was approved by the NERC Board of Trustees on November 5, 2009.

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

> WHEREAS, the NERC Board of Trustees has considered the record of development of a number of proposed interpretations of Reliability Standards, the discussion and recommendations from the November 4, 2009 conference on interpretations, and the recommendation of NERC management,
>
> RESOLVED, that the NERC Board of Trustees approves the following proposed interpretations of Reliability Standards:
>
> 1. Interpretation of Requirement R1 of PRC-005-1;
> 2. Interpretations of Requirement R3 of TOP-005-1 and Requirement R12 of IRO-005-1;
> 3. Interpretation of Requirement R2 of CIP-007-1;
> 4. Interpretation of Requirement R1.3.10 of TPL-002-0;
> 5. Interpretation of Requirements R2 and R8 of MOD-001-1; and Requirements R5 and R6 of MOD-029-1.
>
> FURTHER RESOLVED, that the NERC Board of Trustees provides the following guidance regarding interpretations and the interpretations process:
>
> a. In deciding whether or not to approve a proposed interpretation, the board will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard;
>
> b. It is the expectation of the board that when work on an interpretation reveals a gap or deficiency in a Reliability Standard,

[7] NERC notes the concern highlighted in FERC's July 21, 2008 Order, *Modification of Interchange and Transmission Loading Relief Reliability Standards; and Electric Reliability Organization Interpretation of Specific Requirements of Four Reliability Standards*, 124 FERC ¶ 61,071 (2008), in which FERC approved five modified Reliability Standards and interpretations to five requirements of prior Commission-approved Reliability Standards. In footnote 8 of the July 21 Order, FERC expressed concern that NERC's Rules of Procedure are silent with regard to NERC Board of Trustees approval of interpretations of Reliability Standards. While NERC believes its *Reliability Standards Development Procedure, Version 6.1* addresses the issue, NERC will propose an amendment to its Rules of Procedure to make more explicit the Board of Trustees' expectations to approve interpretations that will thereby address FERC's concern.

stakeholders will take prompt action to address the gap or deficiency in the standard and that the time and effort expended on the interpretation should be a relatively small proportion of the time and effort expended on addressing the gap or deficiency;

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

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

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

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

Therefore, the NERC Board of Trustees, in approving this interpretation, did so using a standard of strict construction that does not expand the reach of the standard or correct a perceived gap or deficiency in the standard. However, the NERC Board of Trustees recommended that any gaps or deficiencies in a Reliability Standard that are evident through the interpretation process be addressed promptly by the standard drafting team. NERC has been so advised, and will further examine any gaps or deficiencies in Reliability Standard CIP-007-2 in its consideration of the next version of this standard through the Reliability Standards Development Procedure. This standard is included in

Project 2008-06 — Cyber Security – Order 706 that is currently targeted for completion by the end of 2010.

IV. CIP-007-2 — Cyber Security — Systems Security Management, Requirement R2

CIP-007-2 requires Responsible Entities[8] to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). FERC approved Reliability Standard CIP-007-2 in its Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing, issued September 30, 2009.[9] In this filing, NERC is submitting a proposed interpretation to Requirement R2, which is labeled as CIP-007-2a and is included in **Exhibit B**. In Section IV (a) below, NERC discusses the interpretation, explains the need for, and discusses the development of, the interpretation to Requirement R2 of CIP-007-2 — Cyber Security — Systems Security Management. Additionally, NERC demonstrates that the interpretation is consistent with the stated reliability goal of FERC-approved Reliability Standards and the requirements thereunder. Set forth immediately below in Section IV(b) are the stakeholder ballot results and an explanation of how stakeholder comments were considered and addressed by the standard drafting team assembled to provide the interpretation.

[8] Within the text of Standard CIP-007, "Responsible Entity" shall mean: Reliability Coordinator; Balancing Authority; Interchange Authority; Transmission Service Provider; Transmission Owner; Transmission Operator; Generator Owner; Generator Operator; Load Serving Entity; NERC; and Regional Entity. The following are exempt from Standard CIP-007-2: Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission; Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters; and Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.
[9] *See* September 30 CIP Version 2 Order.

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

a. Justification for Approval of Interpretation

The stated purpose of Reliability Standard CIP-007-2 — Cyber Security — Systems Security Management is as follows: "Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2." Requirement R2 of this Reliability Standard addresses ports and services necessary for normal and emergency operations. The specific language of this requirement is:

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

> **R2.1:** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
>
> **R2.2:** The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
>
> **R2.3:** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.[10]

[10] Note that CIP-007 Version 1 contains the following language for R2 and R2.3, respectively, that differs slightly from Version 2 language:

R2. **Ports and Services** — The Responsible Entity shall establish and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

On March 9, 2009, the Western Electricity Coordinating Council ("WECC") requested that NERC provide an interpretation of then CIP-007-1 — Cyber Security Systems Security Management, Requirement R2. Specifically, WECC asked whether the term "port" mean[s] a physical (hardware) or a logical (software) connection to a computer. In support of its request, WECC offered the following:

> *The de facto view of the term "port" as used within the standard and within the FAQ has led most organizations to reach the conclusion that "port" is a logical (software) connection to a computer in accordance with most of the application, network and security lexica. For example see the IANA port list at http://www.iana.org/assignments/port-numbers. As such, most organizations have implemented their CIP compliance programs accordingly. If, on the other hand, the view should have been that the term "port" is meant to indicate a physical (hardware) connection to a computer, there may be a very significant effort by many organizations to manually review all physical (hardware). This effort may not be achievable by the respective deadlines within the CIP Implementation Plan resulting in a potential state of noncompliance for a significant segment of the industry, most notably Table 1 and 2 entities that arguably have the largest number, diversity and geographic range of Critical Cyber Assets.*

CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s) and to ensure that only those ports and services required for normal and emergency operations are enabled. The interpretation development team interprets the term "ports" used as part of

---

> R2.3 In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007 Version 2 added a requirement to "document" a process to ensure that ports and services used for normal and emergency operations are enabled in Requirement R2. Additionally, CIP-007 Version 2 removed the "acceptance of risk" language in Requirement R2.3 in accordance with FERC's directive in Order No. 706 at P 600. *See Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC §61,040 (January 18, 2008) ("Order No. 706").

the phrase “ports and services” to refer to logical ports, such as Transmission Control Protocol (TCP) ports, or ports where interface with communication services occur.

NERC believes that the interpretation fairly represents the language in the standard. As presented, the interpretation clarifies what is to be included when considering the term “ports” without expanding the reach of the standard. This clarification helps to assure that the intent of the standard is supported through effective compliance monitoring. Additionally, this interpretation provides clarity and certainty to WECC as it implements its protocols in support of the important reliability objective of ensuring that those ports and services required for normal and emergency operations are enabled.

An interpretation to a standard requirement cannot expand the intent or meaning of the requirement. As such, any modifications to the language in the requirements must be processed through the NERC *Reliability Standards Development Procedure, Version 6.1*. With this in mind, NERC recognizes that increased protection is possible by considering that the term “ports” could include physical ports as well as logical ones. As evidenced by the overwhelming support for the interpretation as proposed, the inclusion of physical ports as well as logical ones was clearly not the intention of this standard. Accordingly, the extension of physical ports in this framework would need to be vetted through the full *Reliability Standards Development Procedure* and made clear in the requirement language in a future update of the standard. Consideration of the inclusion of both physical and logical ports in the requirements of the standard is already included in the scope of Project 2008-06.

b. Summary of the Reliability Standard Development Proceedings

On March 9, 2009, WECC requested that NERC provide an interpretation of then CIP-007-1 — Systems Security Management Requirement R2. NERC assigned its Cyber Security Order 706 Standards Authorization Request ("SAR") drafting team to provide the requested interpretation. The drafting team responded that it interprets the term "ports" used as part of the phrase "ports and services" to refer to logical ports, *e.g.*, Transmission Control Protocol (TCP) ports, where interface with communication services occurs.

In accordance with its *Reliability Standard Development Procedure*, NERC posted its response to the request for interpretation for a 30-day pre-ballot period that took place from August 7 2009 through September 9, 2009. The initial ballot for the interpretation of standard CIP-007-2 — Cyber Security — Systems Security Management Requirement R2 for WECC was conducted from September 9, 2009 through September 21, 2009. There was an 85.31 percent quorum with a 100 percent weighted segment vote. In the comments received, responses to the proposed interpretation were positive. Bonneville Power Administration made the only specific recommendation and suggested changing the term "logical ports" to "logical listening ports." No negative votes were received and the standard interpretation passed on the initial ballot.

V. CONCLUSION

For the reasons stated above, NERC requests that FERC approve the interpretation to Requirement R2 in FERC-approved Reliability Standard CIP-007-2 — Cyber Security — Systems Security Management, as set out in **Exhibit A**, in accordance with Section 215(d)(1) of the FPA and Part 39.5 of FERC's regulations. NERC requests that this interpretation be made effective immediately upon issuance of FERC's order in this proceeding.

Respectfully submitted,

/s/ Holly A. Hawkins

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

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

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 17th day of November, 2009.

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

Exhibit A

Interpretation of Reliability Standard CIP-007-2, Requirement R2
Submitted for Approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

Request for an Interpretation of a Reliability Standard	
Date submitted: March 9, 2009	
Contact information for person requesting the interpretation:	
Name:	Patrick Miller
Organization:	WECC - Western Electricity Coordinating Council
Telephone:	360-567-4056
E-mail:	pmiller@wecc.biz
Identify the standard that needs clarification:	
Standard Number (include version number):	CIP-007-1
Standard Title:	Systems Security Management
Identify specifically what needs clarification (If a category is not applicable, please leave it blank)**:**	
Requirement Number and Text of Requirement: R2 - The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. **Clarification needed:** Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?	
Identify the material impact associated with this interpretation:	
The de facto view of the term "port" as used within the standard and within the FAQ has led most organizations to reach the conclusion that "port" is a logical (software) connection to a computer in accordance with most of the application, network and security lexica. For example see the IANA port list at http://www.iana.org/assignments/port-numbers. As such, most organizations have implemented their CIP compliance programs accordingly. If, on the other hand, the view should have been that the term "port" is meant to indicate a physical (hardware) connection to a computer, there may be a very significant effort by many organizations to manually review all physical (hardware). This effort may not be achievable by the respective deadlines within the CIP Implementation Plan resulting in a potential state of noncompliance for a significant segment of the industry, most notably Table 1 and 2 entities who arguably have the largest number, diversity and geographic range of Critical Cyber Assets.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2009-16: Response to Request for an Interpretation of CIP-007-1 Requirement R2 for the Western Electricity Coordinating Council (WECC)
The following interpretation of CIP-007-1 — Cyber Security — Systems Security Management was developed by the Cyber Security Order 706 SAR drafting team.
Requirement Number and Text of Requirement
R2. The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
Question
Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?
Response
The drafting team interprets the term “ports” used as part of the phrase “ports and services” to refer to logical ports, e.g., Transmission Control Protocol (TCP) ports, where interface with communication services occurs.

Exhibit B

Reliability Standard CIP-007-2a — Cyber Security — Systems Security Management that includes the Appended Interpretation

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2a

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-2:

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

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

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

5. Effective Date: Immediately after approval of applicable regulatory authorities.

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records 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 Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

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

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods,	

		processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
2	05/06/09	Adopted by NERC Board of Trustees	Revised
2a	11/05/09	Added Appendix 2 – Interpretation of R2 approved by BOT on November 5, 2009	Interpretation

Appendix 1

Requirement Number and Text of Requirement
R2. The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
Question
Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?
Response
The drafting team interprets the term “ports” used as part of the phrase “ports and services” to refer to logical ports, e.g., Transmission Control Protocol (TCP) ports, where interface with communication services occurs.

Exhibit C

Complete Record of Development of the Interpretation

Project 2009-16
Interpretation – CIP-007-1, R2 — Systems Security Management

Status:
The interpretation was approved by the NERC Board of Trustees on November 5, 2009 and will be submitted to FERC for approval.

Summary:
The request asks does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?

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

Draft	Action	Dates	Results	Consideration of Comments
WECC Request for Interpretation of CIP-007-1 Interpretation **(2)** Request for Interpretation **(3)**	Initial Ballot Info>> **(4)** | Vote>>	09/10/09 - 09/21/09 (closed)	Summary>> **(5)** Full Record>> **(6)**	
	Pre-ballot Review Info>> **(1)** | Join>>	08/07/09 - 09/09/09 (closed)		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool and Pre-ballot Window
August 7–September 9, 2009

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

Project 2009-16: Interpretation of CIP-007-1 for the Western Electricity Coordinating Council (WECC)

An interpretation of standard CIP-007-1 — Cyber Security — Systems Security Management Requirement R2 for WECC 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 9, 2009**.

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list server for this ballot pool is: bp-2009-16_RFI_WECC_in@nerc.com

Next Steps

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

Project Background

WECC is seeking clarification regarding whether the term "port," as used in Requirement R2, means a physical (hardware) or a logical (software) connection to a computer.

The request and interpretation can be found on the project page:
http://www.nerc.com/filez/standards/Project2009-16_Interpretation_CIP-007-1_WECC.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.

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

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

Request for an Interpretation of a Reliability Standard	
Date submitted: March 9, 2009	
Contact information for person requesting the interpretation:	
Name:	Patrick Miller
Organization:	WECC - Western Electricity Coordinating Council
Telephone:	360-567-4056
E-mail:	pmiller@wecc.biz
Identify the standard that needs clarification:	
Standard Number (include version number):	CIP-007-1
Standard Title:	Systems Security Management
Identify specifically what needs clarification (If a category is not applicable, please leave it blank)**:**	
Requirement Number and Text of Requirement: R2 - The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. **Clarification needed:** Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?	
Identify the material impact associated with this interpretation:	
The de facto view of the term "port" as used within the standard and within the FAQ has led most organizations to reach the conclusion that "port" is a logical (software) connection to a computer in accordance with most of the application, network and security lexica. For example see the IANA port list at http://www.iana.org/assignments/port-numbers. As such, most organizations have implemented their CIP compliance programs accordingly. If, on the other hand, the view should have been that the term "port" is meant to indicate a physical (hardware) connection to a computer, there may be a very significant effort by many organizations to manually review all physical (hardware). This effort may not be achievable by the respective deadlines within the CIP Implementation Plan resulting in a potential state of noncompliance for a significant segment of the industry, most notably Table 1 and 2 entities who arguably have the largest number, diversity and geographic range of Critical Cyber Assets.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2009-16: Response to Request for an Interpretation of CIP-007-1 Requirement R2 for the Western Electricity Coordinating Council (WECC)
The following interpretation of CIP-007-1 — Cyber Security — Systems Security Management was developed by the Cyber Security Order 706 SAR drafting team.
Requirement Number and Text of Requirement
R2. The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
Question
Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?
Response
The drafting team interprets the term “ports” used as part of the phrase “ports and services” to refer to logical ports, e.g., Transmission Control Protocol (TCP) ports, where interface with communication services occurs.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

Request for an Interpretation of a Reliability Standard	
Date submitted: March 9, 2009	
Contact information for person requesting the interpretation:	
Name:	Patrick Miller
Organization:	WECC - Western Electricity Coordinating Council
Telephone:	360-567-4056
E-mail:	pmiller@wecc.biz
Identify the standard that needs clarification:	
Standard Number (include version number):	CIP-007-1
Standard Title:	Systems Security Management
Identify specifically what needs clarification (If a category is not applicable, please leave it blank)**:**	
Requirement Number and Text of Requirement: R2 - The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. **Clarification needed:** Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?	
Identify the material impact associated with this interpretation:	
The de facto view of the term "port" as used within the standard and within the FAQ has led most organizations to reach the conclusion that "port" is a logical (software) connection to a computer in accordance with most of the application, network and security lexica. For example see the IANA port list at http://www.iana.org/assignments/port-numbers. As such, most organizations have implemented their CIP compliance programs accordingly. If, on the other hand, the view should have been that the term "port" is meant to indicate a physical (hardware) connection to a computer, there may be a very significant effort by many organizations to manually review all physical (hardware). This effort may not be achievable by the respective deadlines within the CIP Implementation Plan resulting in a potential state of noncompliance for a significant segment of the industry, most notably Table 1 and 2 entities who arguably have the largest number, diversity and geographic range of Critical Cyber Assets.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Initial Ballot Window Open
September 10–20, 2009

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

Project 2009-16: Interpretation of CIP-007-1 for the Western Electricity Coordinating Council (WECC)

An initial ballot window for an interpretation of standard CIP-007-1 — Cyber Security — Systems Security Management Requirement R2 for WECC is now open **until 8 p.m. EDT on September 20, 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

WECC is seeking clarification regarding whether the term "port," as used in Requirement R2, means a physical (hardware) or a logical (software) connection to a computer.

The request and interpretation can be found on the project page:
http://www.nerc.com/filez/standards/Project2009-16_Interpretation_CIP-007-1_WECC.html

Standards Development Process

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Initial Ballot Results

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

Project 2009-16: Interpretation of CIP-007-1 for the Western Electricity Coordinating Council (WECC)
The initial ballot for an interpretation of standard CIP-007-1 — Cyber Security — Systems Security Management Requirement R2 for WECC ended on September 21, 2009.

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

Quorum: 85.31%
Approval: 100%

Since there was no negative vote with a comment, these results are final. Ballot criteria are listed at the end of the announcement.

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

Project Background
WECC requested clarification regarding whether the term "port," as used in Requirement R2, means a physical (hardware) or a logical (software) connection to a computer.

The request and interpretation can be found on the project page:
http://www.nerc.com/filez/standards/Project2009-16_Interpretation_CIP-007-1_WECC.html

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

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

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

Ballot Results

Ballot Name:	Project 2009-16 - Interpretation - WECC - CIP-007-1 _in
Ballot Period:	9/9/2009 - 9/21/2009
Ballot Type:	Initial
Total # Votes:	209
Total Ballot Pool:	245
Quorum:	**85.31 % The Quorum has been reached**
Weighted Segment Vote:	100.00 %
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.	64	1	49	1	0	0	7	8
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	57	1	44	1	0	0	5	8
4 - Segment 4.	12	1	11	1	0	0	0	1
5 - Segment 5.	44	1	33	1	0	0	2	9
6 - Segment 6.	33	1	25	1	0	0	2	6
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.7	7	0.7	0	0	0	3
9 - Segment 9.	9	0.7	7	0.7	0	0	1	1
10 - Segment 10.	6	0.6	6	0.6	0	0	0	0
Totals	**245**	**7.9**	**191**	**7.9**	**0**	**0**	**18**	**36**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	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	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	City Utilities of Springfield, Missouri	Jeff Knottek		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Abstain	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch		
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Kissimmee Utility Authority	Joe B Watson	Abstain	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	Rodney Hawkins	Abstain	
1	National Grid	Manuel Couto	Affirmative	
1	Nebraska Public Power District	Richard L. Koch		
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura		
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	PacifiCorp	Mark Sampson		
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Affirmative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
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	Abstain	
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Abstain	
1	Tampa Electric Co.	Thomas J. Szelistowski	Abstain	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Westar Energy	Allen Klassen		
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	Affirmative	
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Abstain	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	

3	Alabama Power Company	Bobby Kerley	Affirmative	
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	View
3	City of Farmington	Linda R. Jacobson	Affirmative	
3	City Public Service of San Antonio	Edwin Les Barrow	Affirmative	
3	Colorado Springs Utilities	Alan Laborwit		
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost		
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Abstain	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster	Abstain	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W Pourciau	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen		
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory David Woessner	Affirmative	
3	Lakeland Electric	Mace Hunter	Abstain	
3	Lincoln Electric System	Bruce Merrill		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	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	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson		
3	Santee Cooper	Zack Dusenbury	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt		
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Affirmative	View
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	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	View
5	Calpine Corporation	John Brent Hebert		
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consolidated Edison Co. of New York	Edwin E Thompson	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Robert Smith	Abstain	
5	Entergy Corporation	Stanley M Jaskot	Abstain	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	FPL Energy	Benjamin Church		
5	Great River Energy	Cynthia E Sulzer		
5	JEA	Donald Gilbert	Affirmative	
5	Kansas City Power & Light Co.	Scott Heidtbrink		
5	Lakeland Electric	Thomas J Trickey	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Orlando Utilities Commission	Richard Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp Energy	David Godfrey	Affirmative	
5	Portland General Electric Co.	Gary L Tingley		
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
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 Carolina Electric & Gas Co.	Richard Jones		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Affirmative	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	Black Hills Corp	Tyson Taylor	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Eugene Water & Electric Board	Daniel Mark Bedbury		
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Kansas City Power & Light Co.	Thomas Saitta	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Louisville Gas and Electric Co.	Daryn Barker	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PacifiCorp	Gregory D Maxfield	Affirmative	

6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PP&L, Inc.	Thomas Hyzinski	Affirmative	
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	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	Affirmative	
6	Tampa Electric Co.	Joann Wehle		
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	Dennis Neitzel	Dennis Neitzel	Affirmative	
8	Edward C Stein	Edward C Stein	Affirmative	
8	Encari	Matthew E. Luallen		
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
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	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Service Commission of South Carolina	Philip Riley	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	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	View
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

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

Exhibit D

Interpretation Development Team Roster

Request for Interpretation of CIP-007-01 by WECC Drafting Team — Project 2009-16		
	David L. Norton (Chair)	Entergy
	Jackie Collett	Manitoba Hydro
	Jeri Domingo Brewer	U.S. Bureau of Reclamation
	Gerald Freese	American Electric Power
	John Lim	Con Edison
	Robert Mathews	PG&E
	Kevin B. Perry	SPP
NERC Staff	Scott Mix — Manager Infrastructure Security	North American Electric Reliability Corporation
NERC Staff	Harry Tom — Standards Development Coordinator	North American Electric Reliability Corporation