UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)**	**Docket No. RR06-1-000**

QUARTERLY REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION REGARDING ANALYSIS OF RELIABILITY STANDARDS VOTING RESULTS OCTOBER – DECEMBER 2009

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

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

January 29, 2010

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] submits its fourth quarter 2009 report on the analysis of voting results for Reliability Standards. This filing is submitted in response to the Federal Energy Regulatory Commission's ("FERC") January 18, 2007 Order[2] that requires NERC to closely monitor and report to FERC the voting results for NERC Reliability Standards each quarter for three years. This fourth quarter 2009 report covers balloting results during the October 1, 2009 to December 31, 2009 time frame and includes NERC's analysis of the voting results, including trends and patterns of stakeholder approval of NERC Reliability Standards. This filing completes NERC's compliance commitment.

II. NOTICES AND COMMUNICATIONS

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

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

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

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

[1] NERC has been 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).

[2] *Order on Compliance Filing*, 118 FERC ¶ 61,030 at P 18 (2007).

III. BACKGROUND

NERC develops Reliability Standards in accordance with Section 300 of its Rules of Procedure and the NERC *Reliability Standards Development Procedure*, which is Appendix 3A to the Rules of Procedure.[3] In order for an entity or individual to vote on a proposed Reliability Standard or interpretation ("standard action"), the individual or entity must join the registered ballot body, which includes all entities or individuals that qualify for one of ten stakeholder segments and have registered with NERC as potential voting participants. Each member of the registered ballot body is eligible to participate in the voting process and ballot pool for each standard action. The ten stakeholder segments are:

- Transmission Owners
- Regional Transmission Organizations ("RTOs") and Independent System Operators ("ISOs")
- Load-Serving Entities ("LSEs")
- Transmission Dependent Utilities ("TDUs")
- Electric Generators
- Electricity Brokers, Aggregators, and Marketers
- Large Electricity End Users
- Small Electricity Users
- Federal, State, and Provincial Regulatory or other Government Entities
- Regional Reliability Organizations and Regional Entities

Each standard action has its own ballot pool, populated by interested members of the registered ballot body. The individuals who join a ballot pool respond to a pre-ballot e-mail announcement associated with each standard action. The ballot pool votes to approve or reject each standard action. Specifically, the ballot pool votes determine: first, the need for and technical merits of a proposed standard action; and second, that appropriate consideration of views and objections received during the development process was undertaken.

[3] Version 6.1 of the *Reliability Standards Development Procedure*, effective June 7, 2007, is the latest Commission-approved version.

The *Reliability Standards Development Procedure* process includes three types of ballots: an initial ballot, a recirculation ballot and a re-ballot. If an initial ballot achieves a quorum, but includes at least one negative ballot submitted with comments on the proposed standard action, then a recirculation ballot must be conducted. If an initial ballot does not achieve a quorum, then a re-ballot is conducted using the same ballot pool, but with an extended ballot window.

Approval of a standard action requires both:

- A quorum, which is established by at least 75% of the members of the ballot pool for the standard action submitting a response with an affirmative vote, a negative vote, or an abstention; and
- A two-thirds majority of the weighted segment votes cast must be affirmative. The number of votes cast is the sum of affirmative and negative votes, excluding abstentions and non-responses.

The following process is used to determine if there are sufficient affirmative votes:

- The number of affirmative votes cast in each segment is divided by the sum of affirmative and negative votes cast in the segment to determine the fractional affirmative vote for each segment. Abstentions and non-responses are not counted for the purposes of determining the fractional affirmative vote for a segment.
- If there are less than ten entities that vote in a segment, the vote weight of that segment is proportionally reduced. Each voter within that segment voting affirmative or negative receives a weight of 10% of the segment vote. For segments with ten or more voters, the regular voting procedures are followed.
- The sum of the fractional affirmative votes from all segments divided by the number of segments voting[4] is used to determine if a two-thirds majority affirmative vote has been achieved. (A segment is considered as "voting" if any member of the segment in the ballot pool casts either an affirmative or a negative vote.)
- A standard action is approved if the sum of fractional affirmative votes from all segments divided by the number of voting segments is greater than two-thirds.

IV. SUMMARY OF BALLOTS DISCUSSED IN THIS REPORT

NERC conducted ten ballots from October 1, 2009 through December 31, 2009, each undertaken using the NERC *Reliability Standards Development Procedure*. These ten ballots can be grouped into nine distinct groups of ballot events as follows:

- Interpretation of CIP-001-1, Requirement R2, for Covanta Energy – One (1) Recirculation Ballot

[4] When less than ten entities vote in a segment, the total weight for that segment is determined as one tenth per entity voting.

- Revised Interpretation of CIP-006-1, Requirement R1.1, for Progress Energy – One (1) Initial Ballot

- Interpretation of CIP-005-1, Section 4.2.2 and Requirement R1.3, for PacifiCorp – One (1) Recirculation Ballot

- Violation Severity Levels ("VSLs") for CIP-002-2 through CIP-009-2 and Violation Risk Factors ("VRFs") for CIP-003-2 and CIP-006-2 – One (1) Recirculation Ballot

- Revised Interpretation of EOP-001-0, Requirement R1, for the Regional Entity Compliance Managers – One (1) Initial Ballot

- Revised Interpretation of PRC-004-1 and PRC-005-1 for Y-W Electric and Tri-State Generation and Transmission – One (1) Initial Ballot

- Standards CIP-002-3 through CIP-009-3, a general implementation plan, and a supplemental Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities – One (1) Initial Ballot and One (1) Recirculation Ballot

- Interpretation of BAL-003-0.1b, Requirements R4 and R5, for Energy Mark, Inc. – One (1) Initial Ballot

- Interpretation of CIP-006-1, Requirement R1.1, for PacifiCorp – One (1) Recirculation Ballot

All ten ballots achieved a quorum, and all five initial ballots received at least one negative ballot with comments, initiating the need for a recirculation ballot. Only one of the five initial ballots with at least one negative comment was submitted for a recirculation ballot that was completed during the fourth quarter of 2009. For the other four initial ballots, the drafting teams are reviewing and developing responses to ballot comments before determining the next appropriate action.

No instance occurred where a proposed Reliability Standard or interpretation was disapproved by the ballot pool, and therefore no less stringent versions were approved in a subsequent ballot. The discussion of the detailed ballot results for each ballot event in the fourth quarter 2009 is contained in **Exhibit A** to this filing.

Respectfully submitted,

/s/ Holly A. Hawkins

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

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

EXHIBIT A:

Analysis of 4th Quarter 2009 Reliability Standards Balloting Results

Introduction

On January 18, 2007, the Federal Energy Regulatory Commission ("Commission" or "FERC") issued its *Order on Compliance Filing* ("January 18 Order"),[5] acting on a compliance filing by the North American Electric Reliability Corporation ("NERC") in response to FERC's Order certifying NERC as the nation's Electric Reliability Organization ("ERO") under Section 215 of the Federal Power Act.[6] The January 18 Order requires NERC to closely monitor the voting results for reliability standards and to report to FERC quarterly for three years NERC's analysis of the voting results, including trends and patterns that may signal a need for improvement in the voting process. In its compliance filing in response to the January 18 Order, NERC stated it would file its initial quarterly report with FERC for the first quarter of 2007 and would submit subsequent quarterly filings for the next three years. This is the fourth quarterly report for 2009 and the final report submitted on the analysis of voting results for reliability standards.

Background

The NERC *Reliability Standards Development Procedure* process is administered by action of the NERC Standards Committee. The Standards Committee officially approves the scope and purpose of standards authorization requests, appoints standard drafting teams to develop standards, authorizes field tests of proposed standards when necessary, and approves the proposed standards for ballot. The goal of the *Reliability Standards Development Procedure* process is to gain industry consensus on the need for, and technical sufficiency of, proposed standards. Consensus is primarily established through various formal industry comment periods designed to obtain stakeholder input on the proposed standards. However, interpretations to NERC Reliability Standards proceed directly to the ballot phase as described in the *Reliability Standards Development Procedure* without an industry comment period.

The members of the registered ballot body, comprising entities or individuals registered in one of ten stakeholder segments, must specifically request to be included in the ballot pool for a standard or interpretation ballot event. Any entity or interested individual may become a member of the registered ballot body, but only the ballot pool members are allowed to vote on the proposed standard or interpretation once the balloting begins. If the ballot pool approves a proposed standard or interpretation as described below, the standard or interpretation is presented to the NERC Board of Trustees for its approval and subsequent filing with FERC and applicable governmental authorities in Canada.

[5] *Order on Compliance Filing*, 118 FERC ¶ 61,030 (2007).
[6] *North American Electric Reliability Council and North American Electric Reliability Corporation*, "Compliance Filing of the North American Electric Reliability Council and the North American Electric Reliability Corporation Addressing Non-Governance Issues," *Docket No. RR06-1-000* (October 18, 2006).

The NERC *Reliability Standards Development Procedure* provides for three different types of ballots — an initial ballot, a recirculation ballot and a re-ballot. To "pass," a ballot must achieve a quorum (at least 75% of the members of the ballot pool must return a ballot) **and** must receive an affirmative vote that is at least two-thirds of the weighted segment average of all ballots returned with a vote.

- If a ballot achieves a quorum but includes any negative ballots submitted with comments, then a recirculation ballot must be conducted.
- If a ballot does not achieve a quorum, then a re-ballot is conducted using the same ballot pool, but with an extended ballot window.

There were ten ballots conducted during the fourth quarter of 2009, as shown in the table below; five were initial ballots and five were recirculation ballots. The ballots are discussed below as nine distinct groups of "ballot events."

Ballot Event #	Ballot Name	Initial Ballot Dates	Recirculation Ballot Dates	Ballot Pool Size	Total # of Votes	Quorum	Weighted Segment Approval
1	Interpretation of CIP-001-1 for Covanta Energy (Project 2009-09)		9/29/2009 – 10/9/2009	248	223	89.92%	68.31%
2	Revised interpretation of CIP-006-1 for Progress Energy (Project 2008-10)	9/30/2009 – 10/12/2009		249	199	79.92%	74.47%
3	Interpretation of CIP-005-1 for PacifiCorp (Project 2009-12)		10/16/2009 – 10/26/2009	248	214	86.29%	83.25%
4	VSLs for CIP-002-2 through CIP-009-2 and VRFs for CIP-003-2 and CIP-006-2 (Project 2008-06)		11/2/2009 – 11/12/2009	239	212	88.70%	94.24%
5	Revised Interpretation of EOP-001-0 for the Regional Entity Compliance Managers (Project 2008-09)	11/5/2009 – 11/16/2009		221	190	85.97%	98.07%
6	Revised Interpretation of PRC-004-1 and PRC-005-1 for Y-W Electric and Tri-State G&T (Project 2009-17)	11/19/2009 – 12/7/2009		240	206	85.83%	58.91%
7	Cyber Security 90-day Response – CIP-002-3 through CIP-009-3 and implementation plans – (Project 2009-21)	11/20/2009 – 11/30/2009		240	215	89.58%	88.07%
			12/3/2009 – 12/14/2009	240	224	93.33%	85.55%
8	Interpretation of BAL-003-0.1b for Energy Mark, Inc. (Project 2009-20)	11/20/2009 – 12/7/2009		225	196	87.11%	93.40%
9	Interpretation of CIP-006-1 for PacifiCorp (Project 2009-13)		12/11/2009 – 12/23/2009	252	227	90.08%	78.77%

Discussion of Fourth Quarter 2009 Ballot Events

The first ballot event in the 4th quarter of 2009 consisted of a recirculation ballot for an interpretation of standard CIP-001-1 — Sabotage Reporting, Requirement R2, for Covanta Energy.

On January 26, 209, Covanta Energy requested an interpretation of the term "appropriate parties" and asked if there is an entity within the Interconnection hierarchy that deems parties to be appropriate.

The drafting team offered the following clarifications:

- The drafting team interprets the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. For example, reporting responsibilities result from NERC standards IRO-001 Reliability Coordination — Responsibilities and Authorities, COM-002-2 Communication and Coordination, and TOP-001 Reliability Responsibilities and Authorities, among others. Obligations to report could also result from agreements, processes, or procedures with other parties, such as may be found in operating agreements and interconnection agreements.
- The drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 Requirement R2.
- Regarding "who within the Interconnection hierarchy deems parties to be appropriate," the drafting team knows of no interconnection authority that has such a role.

The recirculation ballot was conducted from September 29, 2009 through October 9, 2009 and achieved a quorum of 89.92% with a weighted affirmative approval of 68.31%. There were 62 negative ballots submitted for the recirculation ballot, and 43 of those ballots included a comment. Some balloters listed more than one reason for their negative ballot.

The reasons cited for the negative ballots included the following:

- Twelve balloters indicated concerns with the references to other standards:
    - Five balloters indicated IRO-001 and TOP-001 have nothing to do with sabotage reporting, with four of those balloters claiming that citing those standards in this way is an indirect interpretation of those two standards and therefore falls outside the ANSI-accredited process. Those four balloters indicated COM-002 is only marginally relevant.
    - Six balloters indicated the references to IRO-001, COM-002-2, and TOP-001 only add confusion and believe the interpretation process should just answer the question asked and not elaborate with further discussion.
    - One balloter indicated that using COM-002 as an example does not provide clarity because COM-002 also uses "appropriate" to describe the entities to which communication should be provided.
    - One balloter indicated the example standards do not address the CIP-001-1 criteria, leaving the entity to make a professional judgment as to whom reports

should or should not be made. The balloter indicated the reporting process should be clearly defined by the drafting team.

- Twenty three balloters indicated concerns regarding the notification of parties for sabotage events:
  - Two balloters indicated Requirement R2 of CIP-001-1 is limited to requiring that the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator and Load-Serving Entity have procedures in place for the communication of information concerning sabotage events.
  - Eight balloters indicated the reference to obligations arising from "agreements, processes and procedures" may be overly inclusive and may encompass contractual or other obligations that are not related to grid reliability.
  - Ten balloters indicated the reference to obligations arising from "agreements, processes and procedures" may fail to include parties that perform one or more reliability functions.
  - Two balloters indicated the list of entities should not be required as auditable evidence in a compliance audit.
  - Six balloters indicated the reference to obligations arising from "agreements, processes, and procedures" is too broad or still undefined.
  - One balloter indicated the interpretation should simply state that the drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1.
  - One balloter indicated the interpretation is not specific enough in its definition of "appropriate parties."
  - Nine balloters indicated either Requirement R2 does not necessitate specific "appropriate entities" to be identified in the procedures or that it should be left to the responsible entity to define the appropriate parties. Most of those balloters stated the list should be determined by the incident and potential impact.
  - Two balloters indicated the notification should be made to the appropriate Reliability Coordinator; one suggested the Reliability Coordinator could cascade the message to other Reliability Coordinators in North America.
  - One balloter indicated the background agreements from which the entities created their lists will not be reviewed during a compliance audit, which will result in an audit simply confirming that the entity has a list for a requirement (R2) that requires an entity have a procedure.
  - One balloter indicated the first part of the interpretation is vague as it implies that the list of these entities should result from requirements of the other standards.
  - One balloter indicated the interpretation needs to be more specific regarding the parties to be communicated with since significant doubt would remain as to whether or not the required communication processes have been established with all necessary parties; the balloter recommended Requirement R2 be revised to explicitly identify parties when CIP-001 is due for its next revision.
  - One balloter indicated "appropriate entities" should be those organizations that need to know given the event and the circumstances. Within an Interconnection,

the entities that should be made aware of the event are the Registered Entity's Reliability Coordinator and/or Transmission Provider(s).

- Four balloters indicated the interpretation still leaves open to debate between auditors and responsible entities the issue of whether the responsible entity identified appropriate interconnection parties.
- Two balloters indicated the third paragraph conflicts with the second. The third says the drafting team knows of no Interconnection authority who deems the parties that are appropriate, but the second says the registered entity must identify the appropriate parties, meaning the registered entity has the authority.
- Two balloters indicated phrases such as "appropriate parties" are ambiguous and would interfere with an auditor's objective audit and could require an auditor (and a registered entity's contracts department) to review every entity contract. This could potentially increase the need for resources for Regional Entities and registered entities with little or no benefit to the reliability of the BES.
- One balloter indicated the response references reporting to entities requiring physical or cyber security event information, but this standard is focused on sabotage.

- Eight balloters indicated general clarification is needed, saying either the interpretation is too vague or does not help with compliance for vague requirements.
- Two balloters indicated the phrase "…those entities to which communication sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 Requirement R2" seems to mean that as long as the reporting entity does what its procedure states then it is in compliance. The balloters claim the purpose of the standards should not only ensure that reporting entities do what they state they will do but that they will perform in accordance with the requirement to maintain an acceptable level of reliability.

The second ballot event in the 4th quarter of 2009 consisted of an initial ballot for a revised interpretation of standard CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets Requirement R1.1 for Progress Energy.

On April 2, 2008, 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 team provided the following 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 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 equivalent or better, to a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to data encryption, and/or circuit monitoring to detect unauthorized access or physical tampering.

The initial ballot was conducted from September 30, 2009 through October 12, 2009 and achieved a quorum of 79.92% with a weighted affirmative approval of 74.47%. There were 46 negative ballots submitted for the initial ballot, and 30 of those ballots included a comment, which initiated the need for a recirculation ballot. Some balloters listed more than one reason for their negative ballot.

The reasons cited for the negative ballots included the following:

- One balloter indicated the interpretation is unnecessary, stating that, based on guidance provided by the National Institute of Standards and Technology ("NIST") for use in its nuclear plants, cabling between physical security perimeters fully contained within an otherwise adequately secured facility is sufficiently protected.
- Two balloters disagreed that wire is a cyber asset. One balloter stated that wiring itself does not possess programmable intelligence and should not require the protection as detailed in CIP-006-1 Requirement R1. The balloter was concerned this level of protection would require entities to make considerable investments into atypical cable protection methods without a corresponding gain in protection of the cyber assets within the ESP or the reliability of the Bulk Electric System.
- Four balloters from the same company indicated they do not fully understand the meaning of the phrase, "Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space."
- One balloter indicated that while the interpretation is politically correct, the use of the Internet is required to exchange market and transmission data to RTOs, and it impossible to prevent hacking.
- Two balloters indicated concern with the use of the term "effective security," stating it does not identify what type of physical protection is equivalent to six-wall borders, and requested clarification.
- Three balloters indicated the interpretation lacks clarity and believe this issue should be addressed during development of the next set of NERC Critical Infrastructure Protection ("CIP") standards.
- Sixteen balloters indicated the interpretation inadvertently results in an expansion of the requirements, which is inconsistent with NERC's *Reliability Standards Development Procedure*.
    - Nine balloters stated that Requirement R1.1 does not specifically discuss wiring nor suggest options that can be used as alternatives to a completely enclosed

("six-wall") border. Some of those balloters further stated that Requirement R3 of CIP-002-1 does not specifically discuss or identify wiring as a cyber asset that would need protection within a six-wall border.

  - Two balloters indicated that use of encryption and other logical access control methods may be sufficient in some cases, but the standard calls for physical protection. Permitting logical measures to control physical access would effectively relax and therefore alter the requirement. One of the balloters suggested the standard be revised to allow alternative protective measures as a future enhancement.
  - One balloter indicated the "FAQ" developed with the original CIP standards specifically states the standards are not intended to address the wires between facilities.
  - Four balloters referenced a number of these types of comments submitted during the initial ballot for the original interpretation response and indicated the only appropriate way to address the issue is via the full standards development process.

- Five balloters indicated the interpretation is not fully responsive to the interpretation request by limiting the response only to wiring.
- One balloter indicated the condition of wiring within the Electronic Security Perimeter that is external to a Physical Security Perimeter should not occur (according to CIP-006-1 Requirement R1.1) and adds a level of complexity to what components/assets are covered and what is expected for compliance.

The third ballot event in the 4th quarter of 2009 consisted of a recirculation ballot of an interpretation of standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3 for PacifiCorp.

On February 6, 2009, PacifiCorp asked the following questions that include reference to Electronic Security Perimeter ("ESP") and Physical Security Perimeter ("PSP"):

1. (Section 4.2.2) "What kind of cyber assets are referenced in 4.2.2 as 'associated'? What else could be meant except the devices forming the communication link?"
2. (Section 4.2.2) "Is the communication link physical or logical? Where does it begin and terminate?"
3. (Requirement R1.3) "Please clarify what is meant by an 'endpoint'? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?"
4. (Requirement R1.3) "If 'endpoint' is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate <u>on</u> the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as 'access points' in addition to the firewalls through which the encrypted traffic has already passed?"

The drafting team provided the following clarifications:

1. In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, *i.e.*, beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
2. The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
3. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
4. In the case where the "endpoint" is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."

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

The reasons cited for the negative ballots included the following:

- Seventeen balloters indicated the interpretation either did not provide sufficient clarity or raised more questions; reasons or examples of their concerns were as follows:
    - Eight balloters sought more information regarding what constitutes an "endpoint" or the communication link's termination points. One suggested the interpretation should state the termination points depend on design and architecture and could include at least three common design examples.
    - Three balloters sought more information about "data communication links."
    - One balloter asked if the communication link was meant to be physical or logical.
    - Four balloters asked how control could be better than a six-wall border.
    - Two balloters gave an example that in the response to question 4, there is discussion relative to layers 3 and higher, but nothing mentioned for layer 1 or 2.
- One balloter disagreed with the response to question 3 regarding logical communication links, stating it could be taken to mean that any device at which a logical connection into the ESP terminates would be considered an access point.
- Thirteen balloters indicated concerns with the answer to question 4:
    - Four balloters indicated the firewall access points already enforce port/protocol restrictions, which meet the requirement, stating that "[a]dding the further restriction of access points at the encryption endpoint is unnecessary, increases complexity which by definition reduces reliability, and can have much wider implications beyond encrypted tunnels."

- Four balloters indicated wording in the response that "the termination points of an encrypted tunnel must be treated as an 'access point'" is too restrictive and will conflict with other interpretations, specifically PacifiCorp's request for interpretation of CIP-006-1. The balloters were concerned that the interpretation could be viewed as indicating all encrypted tunnels are an access point to an ESP.
- One balloter stated that virtual private network ("VPN") traffic should be treated the same as any other logical connection and that the access point to the ESP is able to provide layer 3 and 4 protection regardless of the type of traffic being traversed.
- One balloter indicated the question is confusing but believes the intent is to clarify that "access points" to an ESP can be effectively moved with the application of appropriate equipment. The balloter stated that a communication link between two ESPs utilizing an encrypted tunnel must have an encryption/decryption device at each end inside the ESP that would be defined as the "termination point." The balloter asked, "if an additional protective device is added before the 'termination point' to protect the ESP, would this not affectively move the 'access point?' Must the logs of both protective devices be maintained?"
- Three balloters indicated that "[a] distinction has to be made in the response in regards to the encryption tunnel termination point when deciding whether such termination point is treated as an 'access point' or not."

The fourth ballot event in the 4th quarter of 2009 consisted of a recirculation ballot of proposed VSLs for standards CIP-002-2 through CIP-009-2 and VRFs for CIP-003-2 and CIP-006-2.

Reliability Standards CIP-002-2 through CIP-009-2 were approved by stakeholders and the NERC Board of Trustees, and filed for Commission approval in May 2009. The purpose of this part of the project was to complete the VSLs (for CIP-002-2 through CIP-009-2) and VRFs (for CIP-003-2 and CIP-006-2) for those Reliability Standards. This step is part of the overall Project 2008-06 — Cyber Security Order 706.

- The VSLs are those associated with requirements that were modified when converting standards CIP-002-1 through CIP-009-1 into CIP-002-2 through CIP-009-2.

- The VRFs are for the two Reliability Standards with VRF changes resulting from modifications made during the transition from standards CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2:
  - CIP-003-2 — Cyber Security — Security Management Controls
  - CIP-006-2 — Cyber Security — Physical Security of Critical Cyber Assets.

The recirculation ballot was conducted from November 2, 2009 through November 12, 2009 and achieved a quorum of 88.70% with a weighted affirmative approval of 94.24%. There were 12 negative ballots submitted for the recirculation ballot, and 3 of those ballots included a comment.

The reasons cited for the negative ballots included the following:

- One balloter indicated that the lack of a signed and dated record of the senior manager or delegate(s) annual approval of the list of Critical Assets and Critical Cyber Assets on an

annual basis should not be considered a severe VSL. The balloter stated this is a case where the exposure to penalties focuses on documentation with little to no impact on regional reliability or reducing the risks of wide-spread cascading outages.

- One balloter indicated the assignment of a severe VSL for Requirement R3 of CIP-006-2 for a single Critical Cyber Asset not residing within an identified Physical Security Perimeter is arbitrarily harsh and does not seem to match the violation.
- One balloter indicated the posting lacked clarity regarding scope and reasoning for the changes and stated the drafting team should provide an overview of its work product and approach.

The fifth ballot event in the 4th quarter of 2009 consisted of an initial ballot for a revised interpretation of standard EOP-001-0 — Emergency Operations Planning, Requirement R1, for the Regional Entity Compliance Managers.

On April 2, 2008, the Regional Entity Compliance Managers group submitted a request for an interpretation of EOP-001-0 Requirement R1. Under Requirement R1, the Balancing Authority must have operating agreements with adjacent Balancing Authorities that contain provisions for emergency assistance, including emergency assistance from remote Balancing Authorities. The request asked for clarification on specific terminology and the applicability of Reserve Sharing Group Agreements. This was the second revision of the interpretation. The drafting team revised the interpretation to address balloter concerns regarding (1) application on an Interconnection basis, (2) whether an agreement was required with a remote Balancing Authority, and (3) whether a Reserve Sharing Group agreement could substitute for an emergency assistance agreement with adjacent Balancing Authorities. The questions and responses were as follows:

1. What is the definition of emergency assistance in the context of this standard? What scope and time horizons, if any, are considered necessary in this definition?

   Response: In the context of this standard, emergency assistance is emergency energy. Emergency energy would normally be arranged for during the current operating day. The agreement should describe the conditions under which the emergency energy will be delivered to the responsible Balancing Authority.

2. What was intended by using the adjective “adjacent” in Requirement 1? Does “adjacent Balancing Authorities” mean “All” or something else? Is there qualifying criteria to determine if a very small adjacent Balancing Authority area has enough capacity to offer emergency assistance?

   Response: The intent is that all Balancing Authorities, interconnected by AC ties or DC (asynchronous) ties within the same Interconnection, have emergency energy assistance agreements with at least one Adjacent Balancing Authority and have sufficient emergency energy assistance agreements to mitigate reasonably anticipated energy emergencies. However, the standard does not require emergency energy assistance agreements with all Adjacent Balancing Authorities.

3. What is the definition of the word “remote” as stated in the last phrase of Requirement 1? Does remote mean every Balancing Authority who’s area does not physically touch the Balancing Authority attempting to comply with this Requirement?

   Response: A remote Balancing Authority is a Balancing Authority other than an Adjacent Balancing Authority. A Balancing Authority is not required to have arrangements in place to obtain emergency energy assistance with any remote Balancing Authorities. A Balancing Authority’s agreement(s) with Adjacent Balancing Authorities does (do) not preclude the Adjacent Balancing Authority from purchasing emergency energy from remote Balancing Authorities.

4. Would a Balancing Authority that participates in a Reserve Sharing Group Agreement, which meets the requirements of Reliability Standard BAL-002-0, Requirement 2, have to establish additional operating agreements to achieve compliance with Reliability Standard EOP-001-0, Requirement 1?

   Response: A Reserve Sharing Group agreement that contains provisions for emergency assistance may be used to meet Requirement R1 of EOP-001-0.

The initial ballot was conducted from November 5, 2009 through November 16, 2009 and achieved a quorum of 85.97% with a weighted affirmative approval of 98.07%. There were 5 negative ballots submitted for the initial ballot, and 3 of those ballots included a comment, which initiated the need for a recirculation ballot.

The three balloters, all from the same company, submitting reasons with their negative votes indicated they agreed with most of the changes but had two concerns:

1. The wording in the response to question 2 appears to limit the Balancing Authority to agreements with Balancing Authorities within the same Interconnection, creating a potential for the standard to be interpreted as nullifying the use of existing agreements that cross Interconnections as sufficient to meet this requirement.
2. The phrase "that contains provisions for emergency assistance may be used to meet" does not account for elements of the emergency operations plan that can be deployed in an emergency to alleviate the issue in more lengthy events. The balloters indicated the intent of entities participating in Reserve Sharing Groups is to have Reserves (emergency energy) available to them in the event of such a contingency. Access to “emergency assistance” (emergency energy by this interpretation) is only one aspect of an emergency operations plan.

The sixth ballot event in the 4th quarter of 2009 consisted of an initial ballot of a revised interpretation of standards PRC-004-1 — Analysis and Mitigation of Transmission and Generation Protection System Misoperations and PRC-005-1 — Transmission and Generation Protection System Maintenance and Testing for Y-W Electric Association, Inc. (“Y-WEA”) and Tri-State Generation & Transmission Association, Inc. (“Tri-State”).

On March 25, 2009, Y-WEA and Tri-State requested an interpretation of the term "transmission Protection System" and specifically whether protection for a radially connected transformer protection system energized from the BES is considered a transmission Protection System and is subject to these standards.

The team revised the interpretation based on stakeholder comments submitted during the initial ballot for the first draft of the interpretation. The drafting team prepared the following response:

> The request for interpretation of PRC-004-1 Requirements R1 and R3 and PRC-005-1 Requirements R1 and R2 focuses on the applicability of the term "transmission Protection System." The NERC *Glossary of Terms Used in Reliability Standards* contains a definition of "Protection System" but does not contain a definition of transmission Protection System. The term transmission Protection System is applicable to any Protection System that is installed for the purpose of detecting faults on transmission elements (lines, buses, transformers, etc.) identified as being included in the Bulk Electric System (BES).
>
> In general, a radially connected transformer protection system energized from the BES would not be considered a transmission Protection System. In the event that the transformer low side is connected to a potential source (generator or networked low side system) and there are Protection Systems installed to detect and initiate actions for transmission system faults, then these Protection Systems would be considered transmission Protection Systems.
>
> It should also be noted that due to the variance in the Regional Entity definitions of the BES, specific clarification may be required from the appropriate Regional Entity.

The initial ballot was conducted from November 19, 2009 through December 7, 2009 and achieved a quorum of 85.83% with a weighted affirmative approval of 58.91%. There were 80 negative ballots submitted for the initial ballot, and 46 of those ballots included a comment, which initiated the need for a recirculation ballot. Some balloters listed more than one reason for their negative ballot.

The reasons cited for the negative ballots included the following:

- Four balloters indicated the interpretation could significantly increase compliance enforcement burden with minimal improvement in BES reliability.
- Twenty four balloters indicated concern about references to definitions in the interpretation:
    - Seven balloters indicated the reference to regional definitions of the BES in the last sentence removes the clarity provided by the first two paragraphs. Four of those balloters indicated directing responsible entities to independently seek specific clarification for each Regional Entity is inconsistent with how regional differences have been managed in the standards development processes and does not provide a formal and consistent basis under which responsible entities can demonstrate full compliance with the standard.
    - Two balloters indicated the variance in Regional Entity definitions of the BES should be eliminated by NERC, especially since there are entities that span multiple Regions.

- Five balloters indicated the term "transmission system faults" used in the interpretation needs to be defined. Four of those balloters asked if "transmission system" was synonymous with Bulk Electric System.
- One balloter indicated this interpretation is in conflict with some of the Regional Entities, such as *Reliability*First Corporation.
- Three balloters indicated Regional Entities are going a step further than NERC in the definition of "transmission protection system," which could present a problem in an audit situation.
- Nine balloters indicated the interpretation appears to "define" transmission Protection System, which is inconsistent with the *Reliability Standards Development Procedure* (interpretations may not be used for this purpose).
- Two balloters indicated that, in general, a radially connected transformer protection system energized from the BES would not be considered a transmission Protection System.
- Five balloters indicated that the requestors should address this question at the regional level due to the potential different definitions of a BES based on the region. One balloter explained that the responsibility of defining Bulk Electric System resides with the regions according to both FERC and NERC

- One balloter indicated that due to its transformer configurations the interpretation would incent it to disable protection in order to avoid regulatory risk, an action that would not serve reliability. The balloter suggested the word "normally" be added to a particular phrase (underlined), "In the event that the transformer low side is <u>normally</u> connected to a potential source (generator or networked low side system) and there are Protection Systems installed to detect and initiate actions for transmission system faults, then these Protection Systems would be considered transmission Protection Systems."
- Three balloters indicated the drafting team's response to their comments for the first initial ballot was very helpful, but no corresponding clarification was made to the interpretation for issues relating to "potential sources."
- Two balloters indicated concerns about when the interpretation would go into effect, stating there should be time for entities to include it in their relay maintenance and test program and that the interpretation should not be retroactive to June 18, 2007.
- Fifteen balloters indicated having concerns about the language regarding the classification of system elements (some had multiple concerns):
  - Three balloters indicated the term "networked low side system" is unclear. The balloters suggested revising the phrase to "low side system supplied from multiple transmission substations" to better align with the language regarding radial exclusions in the NERC definition of Bulk Electric System.
  - Four balloters indicated there is no evidence that protection equipment that trips non-BES equipment, such as small networks and generators, poses a threat to the BES. The balloters indicated concern that this definition would non-BES protection systems as transmission protection systems.
  - One balloter stated the revised interpretation still lacked clarity regarding protection systems. The balloter indicated it is possible for (lower voltage) faults on non-BES elements to impact the BES if those faults are not cleared properly;

therefore, any protection system installed with the intention of detecting and initiating action in such cases where the fault is “impactive” should be classified as a transmission protection system.

- Three balloters indicated all transformer taps with low-side voltage below 100 kV should be excluded.
- One balloter indicated the interpretation could inappropriately pull in distribution protection systems, such as 13 kV or 69 kV breakers, on the low side of a transformer.
- Two balloters indicated the interpretation should limit the sub-100 kV Protection Systems that would be considered transmission Protection Systems to those associated with the first protective device downstream from the BES.
- Two balloters indicated the phrase "installed to detect and initiate actions for transmission system faults" needs further clarity. The balloters stated that networked sub-transmission systems (less than 100 kV) may include protection system elements that could “detect and initiate actions for transmission system faults” but are installed to protect the sub-transmission elements.
- One balloter indicated the protection system for a transformer with a high-side voltage greater than 100 kV, connected to a transmission line at greater than 100 kV by a tap, should be considered a BES protection system if (1) the transformer tap connection had two power supplies or (2) the transformer protection system had direct communication with another BES relay or protection system such as a transfer trip system.
- Four balloters indicate there must be a minimum MW value for low-side sources potentially contributing fault energy into the BES. The balloters indicated it does not seem reasonable to include every distributed generation source (no matter the size) and its associated protection schemes in the scope of transmission protection schemes under these standards.

The seventh ballot event in the 4th quarter of 2009 consisted of an initial and recirculation ballot for CIP Reliability Standards CIP-002-3 through CIP-009-3, a general implementation plan, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities*.

The purpose of this project was to modify certain CIP Reliability Standards in response to the directives issued in FERC’s September 30, 2009 Order approving version 2 of the CIP standards. Modifications needed to be filed within 90 days the order, and the Standards Committee authorized deviations from the standards development process to facilitate the schedule. The revised standards include associated VRFs and VSLs.

The initial ballot was conducted from November 20, 2009 through November 30, 2009 and achieved a quorum of 89.58% with a weighted affirmative approval of 88.07%. There were 28 negative ballots submitted for the initial ballot, and 17 of those ballots included a comment, which initiated the need for a recirculation ballot. The recirculation ballot was conducted from December 3, 2009 through December 14, 2009 and achieved a quorum of 93.33% with a weighted affirmative approval of 85.55%. There were 34 negative ballots submitted for the recirculation ballot, and 19 of those ballots included a comment. Some balloters listed more than one reason for their negative ballot.

The reasons cited for the negative ballots included the following:

- One balloter indicated 12 months is not enough time to achieve compliance to the NERC CIP standards for a registered entity's newly identified critical assets, especially for generating stations; the balloter suggested 24 months would be sufficient.
- Four balloters indicated they did not agree with the change to CIP-006 requiring logging each time a visitor exits the Physical Security Perimeter, especially since the visitors are escorted. The balloters suggested that logging a visitor's entry and exit times for the visit should be sufficient.
- One balloter indicated clarification is needed on how to apply a visitor control program for Physical Security Perimeters that have been established at a "cabinet level," such as a situation where the only Critical Cyber Assets, or equipment treated as Critical Cyber Assets per CIP requirements, are housed in a secured cabinet located within a data center. The balloter suggested that since access to the cabinet that houses the Critical Cyber Assets is controlled, the cabinet serves as the Physical Security Perimeter.
- One balloter indicated that physical access logging should be consistent for all types of access (visitors or personnel with authorized unescorted access), and should be covered in one section – Requirement R6 Logging Physical Access.
- Five balloters disagreed with "continuous" escort in R1.6.2 because, in its strictest sense, it requires not letting the visitor out of sight. The balloters suggested reasoning should be applied, and areas with no Critical Cyber Assets and a single access point to the room, *i.e.* bathroom or meeting room, should be exempted. Discretion should be permitted by the responsible person(s) providing the escort to such facilities.
- Five balloters indicated the documentary evidence necessary to prove auditable compliance on every new Critical Cyber Asset at every point in time will likely be unreasonably burdensome.
- Five balloters indicated the implementation plan is unnecessarily complex and should be amended to provide a straightforward way to maintain the Critical Cyber Asset list and demonstrate that changes were appropriate, timely, and compliant.
- One balloter indicated the change to CIP-006-3 Requirement R1.6.1 eliminates the requirement to log the identity of visitors and escorts, effectively reducing clarity and watering down the requirements of the visitor program. The balloter submitted the same comment during the initial ballot and acknowledged the drafting team responded by stating that Requirement R6 (Logging Physical Access) applies to the visitor control program; however, the balloter indicated this is not necessarily clear and believes the requirement must stand on its own merits to prevent ambiguity.

The eighth ballot event in the 4th quarter of 2009 consisted of initial ballot for an interpretation of standard BAL-003-0.1b — Frequency Response and Bias, Requirements R4 and R5, for Energy Mark, Inc.

On April 15, 2009, Energy Mark, Inc. requested clarification regarding Frequency Response, Frequency Bias Settings, and the comparison of the values:

1. Does NERC BAL-003 require every Balancing Authority to have a Frequency Response close to 1% of its projected peak load?

   Response: BAL-003-0.1b does not have a Frequency Response performance obligation.

2. Requirement R2 mandates that each Balancing Authority "establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response". Given the sign convention of the Frequency Bias Setting as applied in the ACE equation, is the Frequency Bias Setting required to be a negative value as close as practical to, or greater than (in absolute terms), the estimated Frequency Response so that AGC will not move resources in a manner that would negate the primary response provided by frequency responsive resources?

   Response: Yes, the Balancing Authority Frequency Bias Setting within the ACE equation is a negative value, expressed in MW/0.1 Hz and should be as close as practical to the natural Frequency Response. If Requirement R2 is met at all times by the Balancing Authority, AGC in Tie Line Bias mode will not move resources in a manner that would withdraw natural Frequency Response.

3. 1) When making the comparison between Frequency Response and Frequency Bias in R2, what is the proper method for this comparison? Should the estimated Frequency Response and Frequency Bias Setting be compared with their typical negative sign convention or in terms of their absolute values? 2) In other words, in order to ensure that AGC does not drive resources to negate the primary response to frequency deviation provided by system resources, including governor response, does Requirement R2 require that the absolute value of the Frequency Bias Setting be as close as practical to, or greater than, the absolute value of the estimated Frequency Response per 0.1 Hz change?

   Response: 1) Frequency Response and Frequency Bias should be compared with their typical sign convention and not an absolute value. 2) Yes, Requirement R2 mandates that the absolute value of Frequency Bias be as close as practical to the absolute value of Frequency Response. Thus, matching Frequency Response and Frequency Bias helps ensure proper AGC performance.

4. Is there any defined measure to determine what "as close as practical" means? Requirement R5 mandates that each Balancing Authority that serves native load shall "have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change. Does Requirement R5 require that the absolute value of the Balancing Authority's monthly average Frequency Bias Setting be at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.

   Response: There is not a defined measure to determine what "as close as practical" means. Yes, Requirement R5 of the standard, as an alternate method of determining a Balancing Authority's Frequency Bias Setting, uses the Balancing Authority's estimated yearly peak demand, or the Balancing Authority's estimated maximum generation level in the coming year for Balancing Authorities that do not serve native load, as a proxy to determine the Balancing Authority's Frequency Bias obligation per 0.1 Hz change. A 1% value of yearly peak demand per 0.1 Hz or 1% value of estimated maximum

generation level in the coming year per 0.1 Hz must be used as the minimum Frequency Bias Setting.

5. As the Frequency Bias Setting is typically calculated and applied as a negative value under R2, yet in R5 it is compared against a percentage of a Balancing Authority's estimated yearly peak demand load and is typically a positive value, is the absolute value of the monthly average Frequency Bias Setting required to be at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change? If not, how does one reconcile the sign convention differences between R2 and R5?

   Response: Yes, the absolute value of the monthly average Frequency Bias Setting is required to be at least 1% of the Balancing Authority's estimated yearly peak demand or at least 1% of the Balancing Authority's estimated maximum generation level in the coming year for Balancing Authorities that do not serve native load.

6. Does BAL-003 have any requirements that would set a value on the amount of Frequency Response that a Balancing Authority must provide?

   Response: BAL-003-0.1b does not have any requirements mandating a specific magnitude of Frequency Response by the Balancing Authority.

The initial ballot was conducted from November 20, 2009 through December 7, 2009 and achieved a quorum of 87.11% with a weighted affirmative approval of 93.40%. There were 13 negative ballots submitted for the initial ballot, and 10 of those ballots included a comment, which initiated the need for a recirculation ballot.

The reasons cited for the negative ballots included the following:

- One balloter indicated the response for clarification 3 is confusing and seems to contradict itself – the first sentence indicates the comparison should be made using the typical sign convention, and the second sentence indicates that Requirement R2 mandates the absolute value of frequency bias be as close as practical to the absolute value of frequency response. The balloter suggested deleting the phrase, "1) Frequency Response and Frequency Bias should be compared with their typical sign convention and not an absolute value," which would enable the remainder of the proposed response to correctly address the requested interpretation regarding Requirement R2.
- Eight balloters indicated the response to item 1 of clarification 3 could be interpreted to conflict with response to item 2. The balloters suggested the response to clarification 3 be reworded to reinforce the significance of the words "or greater than" in Requirement R2 and that the comparison between the Frequency Bias Setting and the average Frequency Response in Requirement R2 must be made comparing the absolute values of the two terms. Four of the balloters suggested the following amended responses:
  - For clarification 3 item 1: "With respect to the comparison of values in Requirement R2, though Frequency Response and the Frequency Bias Setting are negative terms by design, selecting a Frequency Bias Setting as close as practical to, or greater than, the Frequency Response requires comparison of the absolute values of those terms so that AGC in Tie Line Bias mode is less likely to move resources in a manner that would withdraw the primary response provided for a Frequency excursion."

- For clarification 3 item 2: “Yes, Requirement R2 mandates that the absolute value of Frequency Bias Setting be as close as practical to, or greater than, the absolute value of the Frequency Response.”

The ninth ballot event in the 4th quarter of 2009 consisted of a recirculation ballot for an interpretation of standard CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R1.1, for PacifiCorp.

On February 6, 2009, PacifiCorp requested clarification on alternative measures for physical access control:

1. If a completely enclosed border cannot be created, what does the phrase, “to control physical access" require?
2. 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?
3. Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

The drafting team offered the following interpretation:

For 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.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

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

The reasons cited for the negative ballots included the following:

- Three balloters indicated wiring does not qualify as a Cyber Asset subject to CIP requirements. Some balloters offered opinions of what should be considered Cyber Assets:
  - Cyber Assets are those that are IP addressable (routable) or accessible via hard lines (*i.e.* telephone or modem).
  - Cyber Assets are those components to which the wires are connected, such as patch panels, routers, switches, *etc.*
- Five balloters did not believe the interpretation fully addressed the issues raised by PacifiCorp. The balloters indicated the response only addressed the ESP wiring external

to a PSP and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border.

- One balloter indicated the interpretation lacked clarity regarding the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links.”
- One balloter suggested the drafting team explain the purpose of a six-wall border and measures for effectiveness, which would allow for an alternative implementation to be measured.
- Two balloters indicated the question being asked is broader than just the location of the wiring that makes up part of the ESP. One balloter requested more specifics for what constitutes appropriate alternative measures, what is meant by control, and how a logical measure could be equivalent to or better than a physical measure, stating that logical controls won’t prevent a cable from being cut.
- Three balloters indicated the response to question 3 is confusing and introduces ambiguity into the standards, stating a thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.
- Two balloters indicated Requirement R1.1 requires physical measures and does not reference logical measures. One balloter stated that encryption does not control physical access in any way. Though the balloter indicated support for allowing alternative protective measures, both balloters indicated this interpretation would essentially change the requirement and standard, which is inconsistent with the NERC *Reliability Standards Development Procedure* (interpretations may not be used for this purpose).
- One balloter requested clarification regarding whether "wiring" is meant as physical wires or a broader concept of communication paths, “including intermediate devices such as repeaters, bridges, frame relay devices, MPLS nodes, etc.” The balloter also requested clarification regarding which elements of security need to be provided (confidentiality, integrity, availability, *etc*.).
- One balloter seemed to indicate support for this interpretation but voted no with a reference to another interpretation. The balloter indicated this interpretation for CIP-006-1 Requirement R1 clarifies the option to use logical controls as alternative measures, which is something the company supported. The balloter explained the posted interpretation of CIP-005-1, Section 4.2.2 and CIP-005-1, Requirement R1.3, did provide the clarity the company sought regarding the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links.”
- One balloter indicated the response introduces a reference to wiring, but the question did not specifically refer to wiring.
- One balloter indicated concern that this interpretation would make compliance at power plants nearly impossible.
- One balloter indicated the interpretation response inadvertently resulted in expanding the requirements of the standard rather than interpreting the existing requirement. The balloter stated that neither Requirement R1.1 (CIP-006-1) nor Requirement 3 (CIP-002-1) specifically discuss or identify wiring as a Cyber Asset that would need physical protection within a six-wall barrier.

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 29th day of January 2010.

/s/ *Holly A. Hawkins*
Holly A. Hawkins

Attorney for North American Electric Reliability Corporation