NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Recirculation Ballots and Non-binding Poll Open Through 8 p.m. ET Monday, November 5, 2012

Now Available

Recirculation ballot windows for 10 CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, implementation plan, and a non-binding poll for the associated VRFs and VSLs for all 10 standards, are open through 8 p.m. Eastern on **Monday, November 5, 2012**.

Clean and redline versions of each of the ten CIP Version 5 standards (which include CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1), showing changes made since the successive ballot that ended on October 10, 2012, are posted.

The SDT made several minor changes for clarity, consistency, and grammar in each of the standards, none of which were substantive. There were also modifications and additions to clarify particular information in the background, rationales, and Guidelines and Technical Basis sections of certain standards, as well as the change of the name of one defined term (but not the definition itself) from "Intermediate Device" to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. The following summarizes at a high level some of the changes to the requirements:

- **CIP-002-5**: Minor formatting changes in the requirements to clarify that the parts are parts, not sub-requirements (i.e., renumbered from "R1.1", etc., to "1.1", etc., to conform to other standard numbering. Change does not appear in "tracked changes" for redline purposes); clarification of the SDT's intent with respect to kV value connections in attachment 1, criterion 2.5; clarification of the listing of restoration assets for consistency in the requirements and low impact section of attachment 1; and other clarifications in the Guidelines and Technical Basis.

- **CIP-003-5**: Clarification that the one or more policies required by Requirements R1 and R2 must "collectively" include the items listed, and clarification that the "within 30 days" update logically only applies to changes.

- **CIP-004-5**: Clarification for consistency with other standards of the background description of "Medium Impact BES Cyber Systems with External Routable Connectivity." Also clarified in Requirement R1, part 1.1, that the reinforcement of cyber security practices that is required may

include associated physical security practices.

- **CIP-006-5**: Clarification in Requirement R1, part 1.7 that the alarm or alert that must be issued in response to detected unauthorized physical access must occur within 15 minutes of the detection, which is consistent with the subject of the requirement part.

- **CIP-007-5**: Clarification in Requirement R3, part 3.2 in response to uncertainty over what was meant by "identified malicious code" to "detected malicious code," and clarification of Requirement R5, part 5.2 to specify that it only applies to "known" account types, which is consistent with part 5.4.

- **CIP-008-5**: Clarification that reporting to ES-ISAC is required unless prohibited by law and a logical clarification that the report must occur upon determination that a Cyber Security Incident is reportable, as a reportable incident is not identified until it is determined that it is reportable. Also clarified for consistency the time references.

- **CIP-009-5**: Modified "per device capability" to "per Cyber Asset capability" to be consistent with use in other standards and clarified time references for consistency.

- **Implementation Plan**: Minor changes for clarification and consistency, including correction of part references and removal of two illogical references from the initial performance of periodic requirements section, as the performance of those parts are not periodic in nature, but are predicated upon the performance of a different requirement part. Additionally, the SDT provided a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

In addition, the following documents are posted to assist stakeholders in their review:

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Consideration of Issues and Directives – The consideration of issues and directives provides the FERC issues and directives related to the CIP project and the associated consideration by the drafting team.
- Clean and redline versions of the consolidated VRFs and VSLs for all standards, showing changes made since the successive ballot that ended on October 10, 2012.

Instructions

In the recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the recirculation ballot.

The ballot pool for the standards has been cloned to create a ballot pool for a non-binding poll of the associated VRFs and VSLs for all 10 CIP standards. During the non-binding poll window, a comment period is open for comments on the VRFs and VSLs. Please use the electronic comment form to submit specific suggestions for the VRFs and VSLs. (There is no comment period associated with recirculation ballots, therefore, the comment form ask questions specific to the VRFs and VSLs.)

Members of the ballot pools associated with this project may log in and submit their votes for the standards and opinion for the non-binding poll of VRFs and VSLs by clicking here.

Next Steps

If approved, the standards will be presented to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009, with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the

CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management. NERC staff and industry are working together to accomplish this goal in 2012.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com