NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Twelve Initial Ballot Windows Now Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Twelve initial ballot windows, for the following ten CIP standards, the associated implementation plan, and a set of new and revised NERC Glossary definitions, are open through 8 p.m. Eastern on Friday, January 6, 2011.

- CIP-002-5 Cyber Security — BES Cyber Asset and BES Cyber System Categorization
- CIP-003-5 Cyber Security — Security Management Controls
- CIP-004-5 Cyber Security — Personnel and Training
- CIP-005-5 Cyber Security — Electronic Security Perimeter(s)
- CIP-006-5 Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-5 Cyber Security — Systems Security Management
- CIP-008-5 Cyber Security — Incident Reporting and Response Planning
- CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems
- CIP-010-1 Cyber Security — Configuration Management and Vulnerability Assessments
- CIP-011-1 Cyber Security — Information Protection

In addition, the following documents were previously posted to assist stakeholders in their review of the standards:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment/ballot period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)
- Mapping Document – Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 – these 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.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the nonbinding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The nonbinding polls will take place in parallel with the next ballot of these standards.

Instructions for Balloting CIP V5 Standards, Implementation Plan, and Definitions

Each of the ten standards (ten ballots), the associated implementation plan (one ballot), and the set of definitions (one ballot) are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

Members of the ballot pool associated with this project may log in and submit their votes for both the definition and the Detailed Information to Support an Exception Request from the following page: https://standards.nerc.net/CurrentBallots.aspx.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. Please note that comments submitted during the formal comment period and the ballots for the standards all use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

In addition, in consideration of the volume of comments the drafting team anticipates, the drafting team requests that for groups of entities that develop a common set of comments, one member of the group submit the complete set of comments with other members simply submitting a brief statement that they support the comments submitted by [name/affiliation of the member of the group that

submits the complete set of comments]. This is the most efficient way to provide the drafting team with an indication of the volume of support for a set of comments.

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

Next Steps

The drafting team will consider all comments received and determine whether to make revisions to each of the standards, implementation plan, and definitions.

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 directives in FERC Order No. 706.

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 at monica.benson@nerc.net.

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

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