NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Formal Comment Period Now Open: April 12, 2012 – May 21, 2012

Twelve Successive Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: May 11, 2012 – May 21, 2012

Now Available

Ten 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, and a proposed implementation plan have been posted for a formal 40-day comment period through **8 p.m. Eastern on Monday, May 21, 2012**.

CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the Reliability Operations Services according to "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

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

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments submitted during a formal comment period and initial ballots that ended January 6, 2012. Please note that because of the large volume of comments received, the Standards Committee has authorized the SDT to provide detailed summary responses to each question in lieu of the usual practice of providing individual responses to each comment. The SDT believes that the summary responses address all of the comments received, and encourages stakeholders to carefully review the summary consideration in conjunction with the posted redlines. If after reviewing these documents, a stakeholder does not find a response to a comment that they submitted, they may request an individual response

by submitting their request following the instructions below, no later than 5 p.m. Eastern on Friday, April 27. The SDT will provide an individual response within 15 days of receipt of a request.

- 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 forms in Word format – Note that the comment form has been divided into four separate documents to make it more manageable. These correspond to four separate electronic comment forms. The unofficial forms are provided for informal use when compiling responses – the final comments must be submitted through the electronic forms.

Note that the Standards Committee has authorized an extended formal comment period (40 days), with a successive ballot window during the last 10 days of the comment period, in consideration of the large number of Version 5 CIP standards.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Monday, May 21, 2012**. Please use the following comment forms to submit comments.
Comment Form A: CIP-002 and CIP-003
Comment Form B: CIP-004 through CIP-007
Comment Form C: CIP-008 through CIP-011
Comment Form D: Definitions and Implementation Plans

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

Comments must be submitted through the electronic comment forms (links shown above). Due to modifications to NERC's balloting software, voters will no longer able to submit commits via the balloting software.

Instructions for Requesting an Individual Response to a Comment Submitted

After reviewing the Consideration of Comments, a commenter may request additional clarity by using the "Instructions for Requesting Additional Clarity" form included with this notification. Complete the form and submit by email to sarcomm@nerc.net, **no later than 5:00 p.m. Eastern time on Friday, April 27, 2012**.

Next Steps

Twelve successive ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, May 11, 2012 through 8 p.m. Eastern on Monday, May 21, 2011.

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