

## Standards Announcement

### Project 2008-06 Cyber Security Order 706 (CIP Version 5)

#### Initial Ballot Results

#### [Now Available](#)

Twelve initial ballot windows for the following ten CIP standards, one ballot for the associated implementation plan, and one ballot for a set of new and revised NERC Glossary definitions, closed on Friday, January 6, 2011. The drafting team thanks stakeholders for the careful consideration of such a large volume of documents, and for the substantive and constructive feedback received.

Voting statistics for each ballot are listed below, and the [Ballot Results](#) webpage provides a link to the detailed results.

Ballot	Results
CIP-002-5 Cyber Security — BES Cyber System Identification	Quorum: 93.62% Approval: 22.09%
CIP-003-5 Cyber Security — Security Management Controls	Quorum: 93.62% Approval: 33.49%
CIP-004-5 Cyber Security — Personnel and Training	Quorum: 93.62% Approval: 26.82%
CIP-005-5 Cyber Security — Electronic Security Perimeter(s)	Quorum: 93.62% Approval: 28.04%
CIP-006-5 Cyber Security — Physical Security	Quorum: 93.61% Approval: 29.60%
CIP-007-5 Cyber Security — Systems Security Management	Quorum: 93.61% Approval: 24.15%
CIP-008-5 Cyber Security — Incident Reporting and Response Planning	Quorum: 94.02% Approval: 34.30%
CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems	Quorum: 93.61% Approval: 27.28%
CIP-010-1 Cyber Security — Configuration Change Management	Quorum: 93.61% Approval: 26.61%
CIP-011-1 Cyber Security — Information Protection	Quorum: 93.61% Approval: 29.88%
CIP V5 Implementation Plan	Quorum: 92.15% Approval: 42.06%

Ballot	Results
CIP V5 Definitions	Quorum: 92.56% Approval: 25.34%

### Next Steps

The drafting team will consider all comments and determine what changes to make to each of the standards, the implementation plan, and the definitions. After the drafting team has revised the standards, they will be submitted, along with the team's Consideration of Comments, for quality review and subsequently posted for a successive ballot.

### 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.

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. Additional information about the project is available on the [project webpage](#).

### **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](mailto:monica.benson@nerc.net).

*For more information or assistance, please contact Monica Benson,  
Standards Process Administrator, at [monica.benson@nerc.net](mailto: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](http://www.nerc.com)