

Standards Announcement

Informal Comment Period Open

May 4–June 3, 2010

Now available at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Project 2008-06: Cyber Security Order 706 (Phase II)

As authorized by the Standards Committee, the Cyber Security Order 706 Standard Drafting Team requests industry feedback on the initial drafts of CIP-010-1 — Cyber Security — BES Cyber System Categorization and of CIP-011-1 — Cyber Security — BES Cyber System Protection **until 8 p.m. Eastern on June 3, 2010.**

In addition, the drafting team is requesting feedback from industry representatives on whether they prefer the currently proposed format for CIP-011-1, which contains a complete set of requirements; or an alternate format, where the requirements are grouped in separate standards. Industry feedback gathered will be utilized by the drafting team to refine the draft standard for formal industry review in July/August 2010.

Instructions

Please use this [electronic form](#) to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at Lauren.Koller@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Next Steps

Since this is an informal comment period, the drafting team will post the comments received and a summary of how the team used the comments. More information about the scheduling for this project is available in the comment form for this posting. The Standards Committee has authorized the deviations from the current standards development process, such as this informal comment period, to help the team meet its schedule for the delivery of the set of CIP standards.

Project Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these revisions as part of Project 2008-06 — Cyber Security Order 706. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy.

The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

At its meeting on April 13–16, 2010, the SDT agreed that, due to the nature of the proposed changes to the existing CIP standards, the best course of action would be to retire the existing standards and start a new sequence, starting with CIP-010 for the BES Cyber Asset Categorization. The SDT agreed to go forward with one standard (CIP-011) for all of the control requirements for the informal posting, asking for industry input on the comment form on the two format approaches considered.

In response to comments received from a large number of entities to post the requirements for categorization of BES Cyber Systems together with the requirements for the application of controls, the SDT has modified its schedule and intends to ballot the CIP cyber security reliability standards as a single package. In consideration of the very different approach, model, and format used in the drafting of these new CIP cyber security standards, the SDT is proposing a set of two standards in lieu of the original eight standards in the CIP Cyber Security series: CIP-010-1 establishes the foundation for cyber security protection by requiring the identification of what to protect and their categorization; CIP-011-1 establishes baseline cyber security requirements, which must be applied to protect the BES Cyber Systems identified and categorized in CIP 010-1 according their impact category. The alternate format would include CIP-010-1 as described above but would group the baseline cyber security requirements in multiple separate standards numbered consecutively as CIP-011-1, CIP-012-1, CIP-013-1, and so on.

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
Distribution Provider
NERC
Regional Entity

Proposed Glossary of Terms Changes

New terms:

BES Cyber System Component
BES Cyber System
Control Center

Terms to be retired once the standards that use those terms are replaced:

Critical Assets
Critical Cyber Assets
Cyber Assets
Physical Security Perimeter
Electronic Security Perimeter

Standards Development Process

The [Reliability Standards Development Procedure](#) 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 Lauren Koller at lauren.koller@nerc.net*