

Standards Announcement

July 21, 2009

TO: INDUSTRY STAKEHOLDERS

RE: REQUEST FOR INFORMAL INDUSTRY COMMENT REGARDING THE APPROACHES IN THE CONCEPT PAPER “*CATEGORIZING CYBER SYSTEMS — AN APPROACH BASED ON BES RELIABILITY FUNCTIONS*”

Ladies and Gentlemen:

In 2008, the Federal Energy Regulatory Commission (FERC) issued Order 706 paragraph 236 directing the Electric Reliability Organization (ERO) to develop modifications to Reliability Standard CIP-002-1 — Cyber Security — Critical Cyber Asset Identification to address its concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal management approval of the risk-based assessment; (4) the external review of critical assets identification; and (5) interdependency analysis.

On August 7, 2008, the NERC Standards Committee appointed a standards drafting team (SDT) to develop these modifications as part of Project 2008-06 — Cyber Security Order 706. The SDT for the project (CS 706 SDT) was charged to review each of the critical infrastructure protection (CIP) standards and address the modifications identified in [FERC Order 706](#).

CIP-002-2 — Cyber Security — Critical Cyber Asset Identification provides the foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After deliberation, the CS 706 SDT is proposing to revise CIP-002-2 — Cyber Security — Critical Cyber Asset Identification to require a methodology that categorizes BES subsystems and cyber systems according to their impacts on reliability functions. This significant change will benefit the industry by:

- preserving most, if not all, the previous work to protect Critical Cyber Assets under the existing CIP standards;
- eliminating the one-size-fits-all deficiencies of the existing standards;
- simplifying and making uniform the process of asset identification and classification;
- eliminating the need for third-party asset identification oversight;
- improving the overall cyber security of BES assets; and
- minimizing the number of Technical Feasibility Exceptions that an entity would otherwise require for compliance.

This approach is outlined in the concept paper *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*. The concept paper proposes a broader and more comprehensive cyber security approach to protect the systems that support a reliable BES as compared to the requirements contained in the current CIP-002-2 — Cyber Security — Critical Cyber Asset Identification standard.

The CS 706 SDT is seeking informal industry comment on the approaches presented in the concept paper. The CS 706 SDT is requesting comments and suggestions regarding four areas in particular:

- BES reliability functions
- identification of BES subsystems and BES cyber systems
- mapping of BES subsystems
- categorization of cyber systems

Industry input is also requested on the methodology for identification of a “library of security protections” that may be applied to mitigate the risks to the BES.

The informal industry feedback comments provided in response to this posting will be considered by the CS 706 SDT and incorporated, as appropriate, in developing the CIP-002 draft requirements. In the interest of focusing available resources on CIP Version 3 standards development, the SDT will not formally respond to the comments. A subsequent draft CIP-002 — Cyber Security — Cyber Systems Categorization standard will be posted for formal industry comment as part of the ANSI formal standards development process later this year.

The readers of the concept paper are encouraged to use all of their experience during their review, but should be prepared to have their assumptions challenged, as the concepts presented represent a paradigm shift for experienced operating personnel. Cyber security inherently concerns more than a piece of hardware or software or a communication circuit; it encompasses the *system* intimately associated with the reliability functions that it supports.

Due Date and Submittal Information:

The informal comment period is open **until 8 p.m. EDT on September 4, 2009**. Please use this [Word form](#) to submit comments. If you experience any difficulties in using the Word form, please contact Lauren Koller at Lauren.Koller@nerc.net. The informal comment form and concept paper is posted on the project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

*For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*