NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Notes
# Cyber Security Order 706 SDT — Project 2008-06

Thursday, January 28, 2010 from 10:30 am – 4:00 pm Eastern
Conference Number: 1-866-740-1260
Conference Code: 6517897

1. **Administrative Items**
   a. Introductions — All
   b. NERC Antitrust Compliance Guidelines — Howard Gugel
   c. Agenda and Objectives — Phil Huff/Howard Gugel

2. **Brief Status of CIP-002 Standard Development — Phil Huff/Howard Gugel**
   a. Current Posting for Informal Industry Comment
   b. Industry Webinar and Outreach
   c. Consideration of Comments by SDT
   d. Schedule for Formal Posting, Ballot, and BOT Approval

3. **Brief Status of Security Controls Standard Development — Phil Huff/Howard Gugel**
   a. Security Controls Drafting Principles
   b. SDT Subteam Process
   c. Schedule

4. **FERC Staff Questions for Standard Drafting Team**

5. **Standard Drafting Team Questions to FERC Staff**

6. **Next Steps — Phil Huff/Howard Gugel**

7. **Action Items — Howard Gugel**

8. **Adjourn**

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

## Action Items

- FERC to provide feedback to the team as necessary while observing team meetings.
- Regis Binder to look into commission staff providing informal feedback in regard to technical content prior to the formal comment period closing on CIP-002-4.
- FERC and NERC staff to explore policy options in providing formal feedback from the commission.
- FERC and NERC staff to explore options in developing a better approach for allowing entities to apply more appropriate controls while still meeting the compliance objective.

## Introduction

Howard Gugel read the NERC Anti-trust guidelines.

Dave Taylor provided a brief introduction of the meeting objectives. The primary meeting objective was to begin a dialogue between the FERC and the SDT on efforts to address directives from Order 706.

Regis Binder provided opening remarks, stating that FERC has followed the SDT cyber security standards development process within constraints of their limited resources. He also indicated that FERC staff cannot speak on behalf of the commission and they cannot discuss matters related to pending orders by the commission.

## Status of CIP-002 Standard Development

Philip Huff opened by stating that the purpose of the meeting was to foster ongoing communications between the team and FERC staff. He expressed that the project has a tight schedule, and it will be imperative that there is open dialogue throughout the process if the schedule is to be met.

CIP-002-4 was developed to identify and categorize cyber systems related to Bulk Electric Systems (BES) in North America. The standard is posted for an informal industry comment period that ends February 12. Various team members have attended trade organization meetings in order to open a dialogue and encourage participation during the comment period. The team expects to post the standard for a formal comment period toward the end of February. The project schedule calls for the standard to be filed with FERC by June 1.

Philip further stated that the focus of CIP-002-3 was to protect critical cyber systems. In the new version CIP-002-4, the focus is on protecting the reliability of the BES, not necessarily all cyber systems. This idea was presented in a concept paper published to the industry in July, 2009, which was well received. A critical aspect of this process is the development of security controls, which are under development and are expected to be posted in draft form prior to the ballot on CIP-002-4. Additionally, the team had a few targets in mind. The first was to address direction given to NERC in FERC Order 706. The team also wanted to write the standard to minimize the necessity of TFEs.

At this point, the concept of using a cost vs. benefit for risk analysis was discussed. Previously, a "cafeteria" approach (pick what you like and dislike) was used to develop priorities. The team intends to develop justifications for priorities.

The team members have been split into 6 small groups in order to develop the security controls. The teams will finalize their drafts at the March Standard Drafting Team meeting in Phoenix, in order to post drafts in April.

### FERC Questions to SDT

**1) They expressed concern about upstream attacks from low impact targets and how the SDT planned to address these in the Standards. They want to ensure that everything would have at least some minimal baseline of security.**

- D. Batz - How do we not treat the low assets differently than the very high impact assets?
- Dave Norton - Need to preclude the damage a device could do upstream. Protection needs to prevent navigability to higher impact assets.
- Mike Peters – One of the directives in Order 706 dealt with a mutual distrust architecture in the system. Need to create a true mutual distrust where access to a single facility or system does not translate to full access.
- Norton - Need more rigor about how we apply controls to the "weakest link". Prevent upstream attacks to low impact asset.

**2) How is the team using NIST 800-53 with the current compliance program? How do you measure compliance within the NIST Framework?**

*Refer to question #1 of SDT to FERC. The team had also posed this question to the commission staff.*

**3) Order 706 directed regional oversight for the identification of Critical Assets. How do you obtain Regional Oversight in the proposed CIP-002-4?**

- Jim Brenton - We accomplish this through bright-line, objective criteria.
- R. Binder and M. Peters - On their reading, they would agree this meets the directive of oversight.

**4) Regarding the approval of engineering studies by the Reliability Coordinator, do RC's have problems with taking on that responsibility? [Not a concern as much as a question]**

Brenton - A lot of concerns on compliance risk and safe-harbor for RCs

## SDT Questions to FERC

**1) 800-53 is an organizational risk management framework, which allows for tailoring, compensating controls and organizationally defined criteria. However, FERC Order 706 calls for extensive oversight for any exceptions. What are their thoughts on reconciling these seemingly conflicting objectives?**

- R. Binder – Cost/benefit principle is difficult to implement in compliance.
- Scott Wartz – Is this a repackaging of Reasonable Business Judgement?
- Philip Huff – No. Compensating controls still achieve the desired objective. It's not a blanket statement.
- M. Peters – Need to identify the control objective and demonstrate how you meet it.

*Separate discussion*

- M. Peters – Paragraph 152 of Order 706: TFEs is not just technically feasible but also operationally reasonable.
- D. Batz - Uncomfortable with the term "cost". Need to determine the appropriateness and prioritization. Not appropriate to apply same level of protection across every single asset.
- M. Peters - Need to have a minimal level of protection for all of your assets.
- Norton - Brought up "culture of compliance" and difference between "culture of security". It takes auditors that are highly effective.
- Allen Mosher - Fundamentally, this encompasses the approach of results-based standard.

**2) The process to make modifications to the Standards through a FERC Order is very resource intensive. Conversely, changes made prior to industry balloting are relatively cheap. Is it possible to have a process where the team can receive feedback from FERC prior to ballot?**

FERC staff will investigate options for formal input. In addition, FERC staff will attempt to attend future meetings as schedules allow. They have concerns about providing comments about filings that are pending before the commission.

**3) What expectations are there regarding coordination with the Smart Grid CSCTG (Cyber Security Coordination Task Group) product and how we use 800-53/DHS Catalogue?**

- Mike Peters – Look at those interface use-cases they are building. You don't have to match exactly what SG does, but the team should consider participating in the process and provide mutual feedback.

**4) Have we captured all of the directives from order 706 in the filing from December?**

- R. Binder – I don't believe we can comment on this matter since it concerns a pending order.

**5) What are their thoughts about filing CIP-002 separate from the remaining security controls?**

- R. Binder – There are concerns with filing separately
- P. Huff – This shouldn't be a problem because CIP-002-4 does not reference the Security Controls
- D. Taylor – Yes, but they are a suite of Standards. CIP-002-3 would need to be retired.
- D. Batz – The industry would find it difficult doing technical work for a standard [CIP-002-4] that has no effect.
- J. Brenton – At least the industry can begin work on an approved standard in preparation for the security controls.
- M. Peters – This approach is similar to 800-53, right? Are you looking at eliminating CIP-003 through -009?
- J. Brenton – We don't know how it is going to break out. We'll definitely include what's in the current CIP Standards.
- Allen Mosher – Will there be a mapping of changes?
- J. Brenton – Yes
- H. Gugel – We haven't made decisions on format as a team yet.

[*Later discussion: during SDT question period*]

- R. Binder - Conceptually filing separately provides problems. He just wasn't sure what to do with that.
- Dave Taylor – The security controls would follow soon after
- Jan Bargain – You would be posting the security controls informally, right?
- D. Taylor - Yes
- J. Bargain - As long as the plan to marry the two standards, it shouldn't be a problem.
- R. Binder – Not sure that we can approve CIP-002-4 ahead of the security controls.

**6) To what degree can we remove, lessen, or make substitution for prescriptive elements in the current CIP Standard where the risk reduction does not justify the consumption of industry resources in administrative overhead?**

- R. Binder – There would need to be a justification for doing so.
- M. Peters - pg.233 of Order 706 reads that any provisions that would better protect the BES, the Standards Dev. Process has the freedom to so. If the administrative elements actually lessen the reliability of the BES, then we can use that provision.
- Dave Taylor - Requires the SDT to have the type of mapping to demonstrate changes and provide justification anyway.