NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes

Project 2008-06 Cyber Security Order 706 Standard Drafting Team

June 5-7, 2012
Atlanta, GA

Administrative

1. **Introductions and Chair's Remarks**

The chair brought the meeting to order at 8:00 a.m. ET on Tuesday, June 5, 2012 at NERC Headquarters in Atlanta, GA. Meeting participants were:

Members		
Rob Antonishen, Ontario Power	Rene Bourassa, Hydro Quebec (via teleconference)	Jay Cribb, Southern Company
Sharon Edwards, Duke Energy	Jerry Freese, AEP	Christine Hasha, ERCOT
Philip Huff, Vice Chair, AECC	Doug Johnson, ComEd	John Lim, Chair, Con. Edison
Scott Mix, NERC	Steven Noess, NERC Advisor	Robert Lloyd, SCE
David Revill, Georgia Transmission	Kevin Sherlin, SMUD	Thomas Stevenson, Constellation
John Varnell, Tenaska Power Services	William Winters, APS	

Observers		
Janardan Amin, Luminant	Joe Bucciero, EnerNex	Richard Burt, MRO
Bryan Carr, PacifiCorp	David Dockery, AECI	James Fletcher, AEP
Michael Gildea, NERC	Scott Miller, MEAG	Jason Christopher
Summer Esquerre, NextEra	Annette Johnston, MidAmerican	Michael Keene, FERC
Sharon Koller, Alliant Energy	Jason Marshall, Aces Power	Collin Martin, Oncor
Brian Newell, AEP	Dave Norton, FERC	Kevin Ryan, FERC

Observers		
Greg Sims, Southern Company	Monique Tate, NERC	Stacey Tyrewala, NERC
Jennifer White, Alliant Energy	Spencer Young, PacifiCorp	Dan McAveley, Progress Energy
Tom Orvlad, FPL		

2. **Determination of Quorum**

   The rule for NERC Standard Drafting Team (the team or SDT) states that a quorum requires two-thirds of the voting members of the SDT. Quorum was achieved as 15 of 16 total members were present.

3. **NERC Antitrust Compliance Guidelines and Public Announcement**

   The NERC Antitrust Compliance Guidelines and public announcement were delivered.

4. **Review Team Roster**

   The Standards Committee approved the removal of one member from the drafting team on May 24, 2012, as the member changed roles and is no longer able to participate actively in the drafting team's activities. An updated team roster has been posted to the team's project page.

5. **Review Meeting Agenda and Objectives**

   No changes were made to the meeting agenda or objectives. The meeting objectives were to conduct an initial review of industry comments, identify significant unresolved issues, and prepare concepts in response.

Agenda Items

1. **Approval of Notes from Previous Meetings**

2. **Update on Ballot Results and Process Toward Successive Ballot**

   The team reviewed the ballot results from the successive ballot that ended on May 21, 2012, and they discussed topics of disagreement and consensus reflected in the comments. The team will seek to prepare another draft for successive ballot, to be posted in August or September 2012. The team acknowledged that it will need to complete a successive ballot and recirculation ballot before the end of 2012 in order to meet the deadline for filing Version 5 imposed by FERC Order No. 761.

3. **Major Issues and Actions**

   The focus of the meeting was to review the comments and ballot results received during the formal comment and successive ballot period of the second draft posting of the Critical Infrastructure Protection (CIP) standards. The team reviewed major issues from the posting and analyzed on a requirement-by-requirement basis the relative support by commenters of each requirement.

Tuesday and Thursday concentrated afternoon discussions on CIP-002, while Wednesday was devoted to two concurrent sessions: one focused on the issues related to CIP-004 and CIP-006 and the other focused on CIP-005 and CIP-007. Among several issues identified during these meetings for continued team discussion include, but are not limited to:

a. The team generally reviewed Order No. 761 guidance and its implications on the team's work.

b. The SDT discussed with NERC Compliance Operations the concept of internal controls for compliance monitoring. Internal controls are processes, procedures, tools, training, and systems designed to help a registered entity ensure reliability, maintain accountability, and achieve compliance. An entity's internal controls provide auditors a level of assurance, and it is a risk-based approach to compliance with emphasis on:

    i. A compliance approach focused on entity assessment component and shift toward a forward-looking audit program.

    ii. Eliminating zero defect approach to compliance.

c. In broadly discussing the concept of identification of bulk electric system (BES) sites (as opposed to individual facilities, systems, and equipment), the SDT agreed that rather than requiring such granular identification as in current drafts of CIP-002, the focus should be on identifying sites where high and medium impact BES Cyber Systems are, more generally, and then identifying those high and medium impact BES Cyber Systems at those locations. The team determined that more discussion is needed to determine the best approach to this concept, and to ensure that discrete identification of low impact BES sites is not necessary.

d. In context of CIP-004, there is concern that "24 hours" may not meet directive language for "immediate" when describing time allotted for access revocation. Some comments expressed preference for a period longer than 24 hours for access revocation. The SDT continues discussion in determining what time frame will gain industry consensus while also meeting the directive language of Order 706. The comments also indicated that more clarity is needed regarding what access must be revoked, what demonstrates that access is no longer needed, and what starts the clock for "immediate revocation."

e. Added phrase "per device capability" as an alternative to a stricter "where technically feasible." The SDT does not intend for some requirements to require Technical Feasibility Exceptions (TFEs). "Per device capability" is distinct from instances where the requirement requires certain action or performance notwithstanding capability and provides for a TFE. "Per device capability," in contrast with TFE, is used to indicate where a device should meet certain criteria if it is capable, but having that capability is not in and of itself required. The concept of "per device capability" is less onerous and will decrease the need for TFEs in some instances.

f. The team discussed seven year criminal history records check in the context of personnel risk assessment (PRA). The SDT agreed that the focus should pertain to locations "lived" for a period of six consecutive months or more, which may be distinct from (for example) an address of record or official residence. Further clarification is needed to develop the concept, but the team agrees that the concept should eliminate confusion surrounding the tie to school or work that was in the latest draft.

g. Two different controls versus two different systems when establishing a physical security perimeter around critical cyber assets. The SDT clarified in CIP-006 that two or more controls do not require two different control systems. For example, a badge and a PIN are two different controls, but they may be part of one control system.

h. There was discussion concerning disabling unneeded ports versus making them unusable. From a defense in-depth perspective, having multiple security measures will help to provide the level of protection necessary to ensure adequate protection.

i. "Load Serving Entity" (LSE) was eliminated from the applicability section of the standard, as "Distribution Providers" own the assets that are intended to be in scope for the CIP standards. Inclusion of LSE was an unnecessary carryover from previous versions.

j. The team discussed at length the concept of eliminating "zero defect" requirements. The team will continue to review and improve the requirements to eliminate those instances, which is also related to the discussion from NERC Compliance Operations about risk-based approaches to compliance monitoring that focus on internal controls versus measuring individual instances of failure that may not have a reliability benefit. For example, there was general dissatisfaction among commenters about the last draft's attempt to deal with the zero defect issue by the insertion of the 99.99% availability threshold for monitoring systems in CIP-006. Commenters expressed that it will be difficult and potentially costly to quantify and measure 99.9%. The key idea from the team's perspective is that monitoring should be done all of the time, and a response should be initiated promptly upon identification of downtime; however, from a compliance perspective, a loss of monitoring should not in and of itself trigger a violation. The team decided to reassess how terms are used in the applicability columns of CIP-004 – CIP-010 (e.g. Electronic Access Control Monitoring Systems, Protection Control Assets, etc.). The team will continue to discuss in the interim.

k. Annual versus 15 months. The use of both "once per calendar year" and "not to exceed 15 calendar months" caused concern for some commenters. The SDT agrees to use "once every 15 calendar months" which allows for recurrence on a schedule that is generally once per 12 months with flexibility for operational considerations.

4. **Action Items and Next Steps**

   a. Team members were assigned responsibility for completing summaries for individual questions from the comment forms. Summaries must be completed before the beginning of the July 2012 face-to-face meeting.

   b. Participate in all topic-specific SDT interim calls

5. **Future Meeting(s)**

   a. July 10-12, 2012 (Great River Energy in Minneapolis, MN)

   b. August 14-16, 2012 (AEP in Columbus, OH)

   c. September 11-13, 2012 (to be determined)

6. **Adjourn**

   The meeting was adjourned at 4:00 p.m. ET on June 7, 2012. The chair thanked NERC for use of its facilities and thanked the members for a productive session.