NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes

Project 2008-06 Cyber Security Order 706 Standard Drafting Team

February 21-24, 2012
Phoenix, AZ

Administrative

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

The Chair brought the meeting to order at 8:00 a.m. MT on Tuesday, February 21, 2012 at the offices of Arizona Public Service (APS), Phoenix, AZ. Scott Bordenkircher, Director of IT Security and Compliance at APS, provided welcome and opening remarks. Meeting participants were:

Members		
Rob Antonishen, Ontario Power	Rene Bourassa, Hydro-Quebec	Jay Cribb, Southern Company
Sharon Edwards, Duke Energy	Jerry Freese, AEP	Christine Hasha, ERCOT
Philip Huff, Vice Chair, AECC	Doug Johnson, ComEd (via teleconference)	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	William Winters, APS	

Observers		
Janardan Amin, Luminant	Ted Bechtel, US Reclamation	Bryan Carr, PacifiCorp
Jeff Dagle, PNNL	David Dockery, AECI	James Fletcher, AEP
Ameen Hamdon, SUBNET	Annette Johnston, MidAmerican	Michael Keene, FERC
March Myers, NCPA	Brian Newell, AEP	Scott Roe, Corporate Enterprises Security
Rick Terrill, Luminant	Guy Zito, NPCC	Spencer Young, PacifiCorp
Greg Sims, Southern Co	Eduardo Santiago, Southern Co.	Nathan Mitchell, APPA

Scott Stubbs, Oncor		

2. **Determination of Quorum**

   Quorum was achieved for this meeting.

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

   The NERC Antitrust Compliance Guidelines and public announcements were delivered.

4. **Review Team Roster**

   There were no roster changes or updates. There are no vacancies on the drafting team.

5. **Review Meeting Agenda and Objectives**

   No changes were made to the agenda. The objectives of this meeting were to identify and resolve full team issues and common approaches in support of modifying the standards in response to industry comments, and to approve the standards for submission to NERC Quality Review (QR) for successive ballot.

Agenda Items

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

   On February 24, 2012, the team approved the meeting notes from the January 24-26, 2012 meeting.

2. **Update on Process and Key Dates Toward Successive Ballot**

   The team reviewed the near-term project schedule in support of its progress toward revising the Version 5 standards for posting for formal comment and successive ballot. At the end of this (February 2012) meeting, the team plans to submit the standards to NERC QR and to finish its work in responding to the comments received during the initial ballot that ended January 6, 2012.

   The team will meet in March 2012 to consider the feedback from QR and to make final changes before submitting the standards for posting. The team expects to post the standards for posting in early April 2012. In addition, the drafting team requested from the Standards Committee to extend the next formal comment period from the more usual 30-day period to 40-days. The Standards Committee endorsed the team's request on February 14, 2012, and specific details about the request and endorsement are available on the Standards Committee's agenda and notes from that Standards Committee meeting.

3. **Major Issues and Actions**

   a. The following general issues were discussed at the meeting:

      i. Jeff Dagle, of Pacific Northwest National Laboratory (PNNL), presented to the team a review of PNNL's "Analyzing the Power Grid Impacts Resulting from Unintentional

Demand Response."[1] The drafting team requested the presentation in support of the team's discussion and deliberation surrounding the UFLS and UVLS 300 MW thresholds in the latest draft CIP-002-5, Attachment 1, criterion 2.12.

ii. In January 2012, the team considered an issue related to Blackstart Resources and whether CIP-002-5, Attachment 1, should include Blackstart Resources without regard to external connectivity. The team agreed to request discussion from the NERC Operating Committee (OC) and the NERC Planning Committee (PC) on the issue. Certain industry representatives presented a discussion paper to the drafting team, and the drafting team chair provided his perspective in response. Both of those documents were submitted to the OC and the PC and they will be available as part of the OC and PC agenda packages for their March 6 and 7, 2012, meetings. The NERC Standards Development Advisor for the drafting team will attend to introduce both issues to the OC and PC.

iii. The team discussed whether 300 MW is the correct threshold in CIP-002-5, Attachment 1, criterion 2.12. Discussion and input from the PNNL discussion indicates that further research may be necessary. On motion, and approved with 1 abstention, the drafting team agreed to request from the OC and PC a technical study on the MW threshold in CIP-002-5, Attachment 1, criterion 2.12.

iv. At the January 2012 meeting, the team requested feedback from FERC staff on the issue of protecting unneeded ports in CIP-007-5, Requirement R1, Part 1.2 (as reflected in the draft CIP-007-5 from the initial ballot posting).

1. The drafting team proposed to remove that part in response to overwhelming industry feedback that such a requirement is onerous and easily bypassed anyway. Furthermore, CIP-010, Requirement R2, requires configuration change alerts. The team discussed that such alerts combined with the significant changes in requirements relating to perimeter and access security, background investigations, and other means provides an equally effective and efficient alternative to the directive that prompted the requirement part in the first instance.

2. The team provided the following feedback to FERC staff at the January 2012 meeting in support of their request for feedback: "The SDT is persuaded by the industry feedback of the numerous technical, practical, and reliability concerns with this requirement and has removed it. The primary concern was the duplicative nature of the physical access controls required in CIP-006 which already restrict physical access to the assets. The SDT notes that V5 has increased several controls that would further mitigate the risk in this area, such as: physical

[1] The presentation slides were the same as and are available at: http://tcipg.org/news/TCIPG-Seminar-2012-Feb-3-Dagle

security boundaries now require two or more physical access controls for the high impact areas, training requirements for all personnel have been improved and now explicitly cover usage of storage media and security controls, and CIP-010 R2 now requires monitoring and investigation of unauthorized configuration changes. Other issues raised by industry comments include: the difficulty in determining what ports would never be needed for normal or emergency situations and thus could be disabled without harming reliability, the overly burdensome nature of this control in regards to the small risk reduction, the easy bypass of the control by plugging into available ports that are in use, and technical feasibility issues with various devices."

3. A member of FERC staff in attendance at this meeting, who qualified that his opinion does not represent that of the Commission, provided the following feedback, in relevant part, to the team that reflects the opinion of some from the Division of Logistics and Security of the Office of Electric Reliability: unused ports need to be protected, and ports that are necessary should also have some level of protection to ensure that they are not used improperly. Removal of CIP-007-5, R1.2, is an issue for FERC staff, and CIP-010, R2, is not a sufficient substitute, because that is a requirement to detect changes, which is not preventative and only provides after-the-fact notice. Port locks and tamper tape were offered as examples by the FERC staff representative as suggested means that are not onerous (discussion among the team then pointed out that, by the same logic, tamper tape does not disable the port under the requirement language and only provides the same after-the-fact notice that is cited by the FERC staff as insufficient). As a final note, the FERC staff member noted that the posted draft of CIP-007-5, R1.2, only applied to High and Medium Impact Control Centers, and the Commission's Order No. 706 discussed *all* Critical Cyber Assets.

b. The team discussed issues from the comments and proposals for changes in the standards in support of preparing the standards for submission to QR, and, in many cases, they made modifications in response to considering the comments. During the meeting, the following actions were discussed, which culminated in approval of proposals to send each standard to QR along with the associated definitions, implementation plan, and supporting documents. Where indicated, some actions were not approved, but they are noted here to reflect that the team considered it. In each motion to send a standard to QR, the motion included instruction to approve the associated definitions (except where indicated), to make conforming changes to the Violation Severity Levels, to carry over from CIP-002-5 the agreed-upon applicability section, and to make edits for consistency, style, form, and grammar.

    i. In CIP-002-5, Attachment 1, remove "2.4" from criteria 1.2 and 1.4 and add the reference to criterion 2.13 instead. Motion approved with 5 abstentions.

ii. In CIP-002-5, Attachment 1, criterion 2.12, change the 300 MW threshold to 1500 MW. Motion *not approved,* with 7 opposed and 4 abstentions.

iii. In CIP-002-5, Attachment 1, criterion 2.12, request from the NERC Operating Committee and Planning Committee a study on an appropriate MW threshold compared to the 300 MW in the criterion. Motion approved with 1 abstention.

iv. In CIP-002-5, Attachment 1, criterion 2.4, add "connectivity" as a condition for inclusion with regard to Blackstart Resources. Motion *not approved*, with 5 opposed and 3 abstentions.

v. Advance CIP-002-5 to QR, pending further discussion on Control Center. Motion *not approved* with 5 opposed.

vi. Advance CIP-003-5 to QR. Motion approved with 1 abstention.

vii. Approve changes made to Control Center definition. Motion approved with 3 abstentions.

viii. After approving the changes made to Control Center, the team reconsidered CIP-002-5 in light of the changes. Advance CIP-002-5 to QR, subject to conforming changes to Violation Severity Levels, guidance, and style, form, and grammar. Motion approved with 3 opposed.

ix. Advance CIP-004-5 to QR. Motion approved with 1 abstention.

x. Advance CIP-005-5 to QR. Motion approved with 1 opposed and 3 abstentions.

xi. Reinstate CIP-007-5, Requirement R1.2 from initial posting, as amended. Motion approved with 2 opposed and 2 abstentions.

xii. Retain applicability to Control Centers in CIP-007-5, Requirement R1.2 (with regard to Medium Impact BES Cyber Systems, instead of applicable generally to all Medium Impact). Motion approved with 1 opposed and 1 abstention.

xiii. Change "log" to "store" and add "and logged" in CIP-007-5, Requirement R4.1. Motion approved with 1 abstention.

xiv. Advance CIP-007-5 to QR. Motion approved unanimously.

xv. Advance CIP-008-5 to QR. Motion approved unanimously.

xvi. Advance CIP-009-5 to QR. Motion approved unanimously.

xvii. Advance CIP-10-1 to QR. Motion approved unanimously.

xviii. Advance CIP-011-1 to QR. Motion approved with 3 abstentions.

xix. Advance CIP-006-5 to QR. Motion approved with 3 opposed and 2 abstentions.

xx. Advance the CIP Version 5 Implementation to QR. Motion approved unanimously.

xxi. Approve meeting notes from January 24-26, 2012. Motion approved unanimously.

4. **Action Items and Next Steps**

   a. Complete and submit to the NERC Standards Development Advisor all considerations of comments, to include individual comment replies and question summaries, no later than Friday, March 2, 2012. Question summaries should identify all issues raised by commenters, along with action taken in the standards.

   b. Review and submit any changes, as necessary, to the Violation Risk Factor/Violation Severity Level justifications by Friday, March 2, 2012.

5. **Future Meeting(s)**

   The next face-to-face meeting will be Tuesday, March 20, 2012 |8:00 a.m. CT through Thursday, March 22, 2012 |6:00 p.m. CT at the Arkansas Electric Cooperative Corporation facilities in Little Rock, AR. Details will follow.

6. **Adjourn**

   The chair thanked APS for their hospitality and adjourned the meeting at 11:00 a.m. MT on Friday, February 24, 2012.