NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706

36th Draft Meeting Summary

Salt Lake City, UT

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

to ensure the reliability of the bulk power system

July 19-21, 2011

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

Table of Contents

MEETING SUMMARY

John Lim, chair of the Cyber Security Order 706 (CSO 706) Standard Drafting Team (SDT) welcomed members and other participants to the Salt Lake City Meeting of the CSO 706 SDT, and he thanked them for their participation in this meeting. John also acknowledged and thanked Brandy Daniels, the meeting space coordinator and hostess, and the Western Electric Coordinating Council (WECC) for all of their efforts in making the meeting possible. Brandy reviewed the meeting logistics and safety information. At the beginning of each day, Joe Bucciero, NERC Facilitator, conducted a roll call and reviewed the public meeting notices, and Steven Noess, NERC Standards Development Advisor, reviewed the NERC antitrust guidelines.

The chair outlined the meeting objectives the SDT sought to accomplish by the end of this meeting: (Agenda Package - see ***Appendix 1***)

1. Reviewing and walking through substation and generation facility diagrams to review application of the draft Version 5 standards,
2. Identifying any potential questions and issues to discuss in a meeting with the Federal Energy Regulatory Commission (FERC) on July 28, 2011 in Washington, D.C.,
3. Reviewing and refining any changes to Version 5 drafts of the CIP-002 through CIP-011 requirements, reviewing the preliminary implementation plan, VSLs/VRFs, and guidance documents, and agreeing on the team's next steps and assignments.

The chair reported on the changes approved by the NERC Standards Committee (SC) to the membership of the drafting team. These changes are:

1. The addition to the drafting team membership of René Bourassa from Hydro Québec and;
2. The resignation of Joe Doetzl, John van Boxtel, and Scott Rosenberger.

Industry Review

- Scott Mix and John Lim provided an update on other industry activity regarding cyber security.
- John Lim reported on the Cyber Attack Task Force activities – no real changes since the last report.
- John Lim reported that the DOE/NIST/NERC Risk Management Process is planning a late August posting of its initial findings.
- Scott Mix reported that the industry survey results for FERC (RM-11-11) are being prepared for filing.

Drafting Team Schedule

The drafting team reviewed the current project and meeting schedule (See ***Appendix #4***), and the team discussed upcoming meeting dates, objectives, and locations. The team confirmed that the August 2011 meeting will be an open session with representatives from industry organizations in Atlanta, GA, at NERC's new headquarters facilities to review an in-progress draft of Version 5 of the CIP Cyber Security Standards. The team also targeted the September 2011 meeting to finalize the CIP standard drafts needed to begin the quality review and posting process, with a target date of initial posting of the Version 5 standards in early November 2011.

Subteam Assignments

The drafting team agreed that at least for the next couple of weeks, the full drafting team should participate in the interim conference calls to finalize the next draft of the Version 5 standards in time for the August 2011 meeting with the industry representatives.

Needs, Goals, & Objectives

The drafting team was reminded of the Needs, Goals, and Objectives it previously developed (see ***Appendix #5***)

CIP Version 4 Impact

Rich Kinas agreed to provide a summary of the results of his company's analysis of the survey results data. The draft presentation offered by Rich at this meeting can be found in **Attachment 8**. The presentation of aggregated data contained within NERC's official response to a particular FERC data request visually demonstrated resources by type and rating across the different regions. The data also showed a breakdown of non-critical assets, critical assets without cyber critical assets, and critical assets with critical cyber assets. The drafting team found the data useful, especially in conjunction with the Overview of Scenarios conducted later by Dave Revill and Jim Fletcher. The presentation showed, in some instances, key differences among regions with regard to types or ratings of facilities.

Drafting Subteam Reports

Each of the drafting subteams provided a summary report of their current status regarding their revisions to the specific requirements assigned to them, and each of the teams, along with the full drafting team, will continue to meet over the next few weeks to continue to work on their respective draft requirements. A copy of the latest drafts incorporating changes from this meeting and subsequent conference calls will be sent out after close of business on August 5, in clean version, to industry stakeholder organizations in preparation for the August 2011 SDT meeting in Atlanta, GA.

Overview of Scenarios

Team member Dave Revill and Observer Jim Fletcher provided the drafting team with detailed overviews of how the draft Version 5 CIP standards might impact and correspond to operations and devices at typical substation (Attachment #9) and generation facilities (Attachment #10). As part of their presentation, they presented diagrams of facilities, lists of equipment common at each type of facility, and a detailed spreadsheet that identified each component of each

requirement and associated concerns, where appropriate, of difficulties or issues entities might have in implementing certain aspects of CIP Version 5. Much of the discussion related to specific examples of operational realities and how a particular requirement might or might not best address that scenario.

The drafting team found the discussion incredibly useful, and each of the subteams noted concerns to make adjustments as needed in the corresponding standards.

External Connectivity and Electronic Access Point

With the aid of the diagrams and associated discussion surrounding the substation and generation facilities, the team identified unresolved concerns relating to the proposed definitions of "external connectivity" and "electronic access point" that are being used in various places throughout CIP Version 5.

For the remainder of the second day and most of the third day of the meeting, the team made significant progress in identifying concerns with the proposed definitions and their ensuing impact on particular requirements in the draft Version 5 requirements. In response to much discussion and debate along with a general sense by the team of what concepts needed addressing, Jay Cribb agreed to take up the issues upon adjournment and to develop straw man definitions and discussion points for the team to continue refining in the conference call meetings that will follow this SDT meeting.

Subteam Review of Latest Version 5 CIP Standards

Among the several general issues identified in response to day two and day three discussions are the following:

- The drafting team should consider the inclusion of a mapping in the guidance document between the reliability functions and the functional model as part of guidance for CIP 002. Given the work being done by the BES Definition drafting team, a change should be considered to use the term "reliability tasks" instead of the term "reliability functions" so as to completely disconnect the terms and minimize any possible confusion with the NERC Functional Model.
- Further discussion is needed regarding "ownership" vs. "operational responsibility" with respect to identifying the entity that is responsible to implement the changes needed for compliance with the CIP standards.
- It would be useful to have a document showing process flow (e.g., Gen Examples from Salt Lake City (SLC) SDT meeting) and evidence required to comply with the standards, which might be helpful in identifying assets that are within scope.
- Continue work on establishing process for how to define BES Cyber Systems.
- Additional guidance on the criteria in CIP-002 should be considered for what constitutes BES Cyber Systems as well as their categorization into High, Medium, or Low impact. Do we need a list of all Low Impact assets? Preferably not.

- Additional discussion/justification is needed concerning the criterion of 3 or more 300kV lines at a station or substation vs. stations or substations that are operated at 200kV.
- Be clearer on definitions regarding electronic access points, especially in conjunction with CIP 005. This will assist in developing thresholds for what BES Cyber Asset or BES Cyber System is in or out of scope for particular standards and associated requirements.
- More thought is needed to describe the requirements for password strength. Also is encryption needed across untrusted networks?
- Identify places where "external connectivity" is used and determine if it needs to have "routable" or "non-routable" distinctions. (e.g., CIP 005-5, R1.4)
- For Generation and Substations – Consider that with no external connectivity, how to perform quarterly reviews?
- Generation and Substations - Changing the shared password should not be required for revocation if the account cannot be used to access the system remotely.
- Assumptions/scenarios for Electronic Access (basis for the work that Jay Cribb will continue to lead):
    - Connectivity characteristics not the relevant factor, but what functionality can be accomplished with or without that connectivity.
    - Work on Definition of external connectivity. Regardless of what the particular device is connected to, is it reachable from outside the electronic access perimeter? Connectivity vs. routable connectivity.
    - CIP-006-5, R1.4: Is physical protection required on Medium Impact if no external connectivity exists for the BES Cyber Asset or BES Cyber System?
    - How do we prove we have controlled access (e.g. serial)?
    - Address (exclude w/o excluding relevant communications) communication assisted tripping
    - Keep documentation requirements manageable; identify by classes of devices/connections
    - Wholly-owned communication network, and impact of location of firewall, e.g., for risk based assessment
    - BES Cyber Asset vs. non-BES Cyber Asset Connectivity - is a serial vs. non-serial distinction needed?
    - Impact of protection on reliability and performance.

At the conclusion of the SDT's review of the latest draft of the CIP V5 Standards, the team generated a set of draft questions that the team has of the FERC Technical Staff. These questions will be forwarded to the FERC Technical Staff in preparation of the meeting with the drafting team scheduled for July 28, 2011 in Washington, DC. (**Attachment #6**)

Interim Conference Calls

The drafting team established several interim conference calls following the Salt Lake City meeting to lead up to the August 2011 meeting in Atlanta. In response to individual scheduling conflicts causing less participation on individual subteam meetings, the drafting team agreed that the interim calls should aim to have full participation, to the extent possible, by the drafting team.

A schedule was developed to address individual subteam topics, but all members were asked to attend. Meetings will occur for two hours, four days a week, for the two weeks leading up to the August 2011 meeting. Having more of the drafting team available for each of the calls will also enable more of the team to be involved in proposed changes to the requirement drafts, thereby allowing more of the agenda during the drafting team meeting in August 2011 to be devoted to industry feedback.

Action Items

1. Jay Cribb will provide definitions for connectivity
2. Rich Kinas/John Lim will continue to work on the Criteria for CIP-002
3. Jerry Freese will review and provide wording for Electronic Access for CIP-004
4. Doug Johnson will review and provide wording for Physical Access for CIP-004/006
5. John Lim/Steve Noess will review the CIP standards vs. FERC Order 706 for completeness and will update the Applicability entries in the requirements as appropriate
6. Joe Bucciero will send the agenda for the August 2011 Meeting to the PLUS List and will check with Holly and Elizabeth at NERC about sending it to the industry organization representatives.
7. Joe Bucciero/Steve Noess will check with Eleanor at NERC on the meeting registration list for the August 2011 meeting.

Adjournment

The Chair thanked everyone for attending this meeting, either in person or via the conference call facilities, and he expressed appreciation on behalf of the drafting team to Brandy Daniels for her excellent job in coordinating meeting space and hosting the team at WECC.

The Meeting Evaluation Survey results are included as **Attachment #7**.

The meeting adjourned at approximately 4:30 p.m. on Thursday, July 21, 2011.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda – Appendix 1
Project 2008-06 Cyber Protection Order 706

36th Drafting Team Meeting
Meeting Location: Western Electric Coordinating Council (WECC)
155 North 400 West
Salt Lake City, Utah

Tuesday, July 19, 2011 | 8:00 a.m. – 6:00 p.m. ET

Proposed Meeting Objectives/Outcomes

1. To determine feasibility of applying requirements in example generation and transmission facilities
2. To capture guidance for applying requirements in example generation and transmission facilities
3. To review modifications made to requirements based on auditor feedback
4. To review initial draft of implementation plan
5. To discuss strategy for drafting VSLs and VRFs
6. To agree on next steps and assignments

Agenda

8:00 Introduction, Welcome, Opening and Host remarks - **John Lim, Chair & Phil Huff, Vice Chair**
Roll Call; NERC Antitrust Compliance Guidelines - **Joe Bucciero, NERC**

8:15 Review of meeting objectives and agenda - **John Lim**

8:30 Industry Updates - **Scott Mix, NERC, Mike Keane, FERC and others**

- Cyber Attack TF Report
- DOE/NIST/NERC Risk Management Process
- Other Cyber Security business

9:00 Review results of industry survey - **Scott Mix**

9:30 FERC Meeting and August Meeting

10:00 **Break**

10:15 Review modifications made to CIP-002-5 - **John Lim**

12:00 **Lunch**

1:00 Review modifications made by Recovery and Response Sub-Team – **Tom Stevenson**

2:00 Review modifications made by System Security Sub-Team – **Jay Cribb/Christine Hasha**

3:00 **Break**

3:15 Review modifications made by Access Control Sub-Team **– Roger Fradenburgh/Philip Huff**

4:00 Review modifications made by Physical Security Sub-Team – **Doug Johnson, ComEd**

5:00 Review modifications made by Governance Sub-Team – **Dave Revill**

6:00 **Recess**

Wednesday, July 20, 2011 | 8:00 a.m. – 6:00 p.m. ET

Agenda

8:00 Recap of Day 1, Agenda Review, Roll Call and Antitrust **Guidelines – John Lim, Philip Huff, Joe Bucciero**

8:15 Overview of Scenarios – **Jim Fletcher/Dave Revill**

9:00 Identify Generation BES Cyber Systems

10:30 **Break**

10:45 Identify Transmission BES Cyber Systems

12:15 **Lunch**

1:15 Walk-through CIP-004-5 Access Authorization and Revocation

2:15 Walk-through CIP-005-5 R1 (ESP)

3:00 **Break**

3:15 Walk-through CIP-007-5 R1 Ports and Services

4:15 Walk-through CIP-007-5 R2 Security Patch Management

5:00 Walk-through CIP-007-5 R3 Malicious Code Prevention

6:00 **Recess**

Thursday, July 21, 2011 | 8:00 a.m. – 5:00 p.m. ET

Agenda

8:00 Recap of Day 1, Agenda Review, Roll Call and Antitrust Guidelines – **John Lim, Philip Huff, Joe Bucciero**

8:15 Schedule Interim Meetings

8:30 Walk-through CIP-007-5 R4 Security Event Monitoring

9:15 Walk-through CIP-007-5 R5 Access Control

10:00 **Break**

10:15 Walk-through CIP-007-5 R6 Maintenance

11:00 Walk-through CIP-010-5 R1 Configuration Change Management

11:45 **Lunch**

12:45 Walk-through CIP-010-5 R3 Vulnerability Assessments

1:45 Walk-through CIP-011-5 R2 Media Reuse and Disposal

2:30 **Break**

2:45 Review Implementation Plan Straw-Man

3:45 Discuss VSLs/VRFs

4:15 Discuss Additional Guidance within the Standard

4:45 Review Next Steps

5:00 **Adjourn**

Appendix 1-CSO 706 SDT Consensus Guidelines

(Adopted, November, 2008, Revised June 2010, Revised July, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined - Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least two thirds favorable vote of all members present and voting.

Quorum Defined - The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).
2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.

4. Electronic voting results will be recapped at the beginning of the next regular meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 2/3's voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

Appendix 2: Meeting Attendance - July 19-21, 2011

Members Attending
In Person or via ReadyTalk and Phone

Name	Company	July 19	July 20	July 21
1. Rob Antonishen	Ontario Power Generation	X	X	X
2. Jay Cribb	Southern Company Services	X	X	X
3. Gerry Freese	AEP	X	X	X
4. Christine Hasha	ERCOT	X	X	X
5. Philip Huff, Vice Chair	Arkansas Electric Coop Corporation	X	X	X
6. Doug Johnson	Exelon Corporation – Commonwealth Edison	X	X	X
7. Rich Kinas	Orlando Utilities	X	X	X
8. John Lim, Chair	**Consolidated Edison Co. NY**	**X**	**X**	**X**
9. Robert Preston Lloyd	Southern California Edison	X	X	X
10. David Revill	Georgia Transmission Corporation	X	X	X
11. Kevin Sherlin	Sacramento Municipal District	X	X	X
12. Tom Stevenson	Constellation	X	X	X
13. John Varnell	Tenaska	X	X	X
14. William Winters	Arizona Public Service.	X	X	X
Joe Bucciero	NERC Facilitator	X	X	X
Roger Lampila	NERC Staff	X	X	X
Scott Mix	NERC Staff	X	X	X
Steve Noess	NERC Staff	X	X	X

Observers

Participant	Affiliation
Sharla Artz	SEL
Jan Bargen	FERC
Kathy Daggett	MidAmerican Energy
Matt Dale	FERC
David Dockery	AECI
Jay Doran	MidAmerican Energy
Joe Doetzl	CRSI
Jim Fletcher	AEP
Kuldeep Hak	SCE
Michael Keane	FERC
Kim Koster	MidAmerican Energy
Barry Kuehnle	FERC
Andres Lopez	Corp of Engineers
Daniel Moore	WFEC
Martin Narendorf	CenterPoint Energy
Brian Newell	AEP
Scott Rosenberger	Energy Future Holdings
Katie Schnider	SEL
Justin Searle	UtiliSec
Melissa Wehde	MidAmerican Energy
Bryn Wilson	Oklahoma Gas & Electric
Guy Zito	NPCC

Appendix 3: Project 2008-06 Drafting Team Roster

1.	**Chair**	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York
2.	**Vice Chair**	Philip Huff Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation
		Members	
3.		Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc.
4.		René Bourassa	Hydro Québec
5.		Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc.
6.		Sharon Edwards Project Manager	Duke Energy
7.		Gerald S. Freese Director, NERC CIP Compliance	American Electric Power
8.		Christine Hasha Compliance Analyst Senior	Electric Reliability Council of Texas
9.		Jeffrey Hoffman Chief Architect, IT Policy and Security Division	U.S. Bureau of Reclamation Denver Federal Center

10.	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon – Commonwealth Edison
11.	Robert Preston Lloyd Sr. Technical Specialist, Substation Regulatory Compliance	SC&M Technical Support & Strategy Southern California Edison
12.	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission
13.	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation
14.	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District
15.	Thomas Stevenson General Supervisor Engineering Projects	Constellation Energy
16.	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology
17.	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co.
18.	William Winters IS Senior Systems Consultant	Arizona Public Service Co.

Consultant to NERC	Joseph Bucciero Standards Development Coordinator	Bucciero Consulting, LLC
NERC Staff	Tom Hofstetter Regional Compliance Auditor	North American Electric Reliability Corporation
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation
NERC Staff	Steven Noess Standards Development Advisor	North American Electric Reliability Corporation
NERC Staff	Andy Rodriquez Director of Standards Development	North American Electric Reliability Corporation

Appendix 4: Cyber Security Order 706 - Project Schedule (July 2011)

Meeting Location	Dates	Meeting Objective
Salt Lake City, UT WECC	**7/19 - 7/21/2011**	**Walk-through sample generation and substation environments with the Version 5 requirements to determine feasibility. Output additional guidance based on the walk-through process**
Interim	7/22 - 8/15/2011	Revise drafting requirements based on feedback from walk-through process – **primarily agree to the use of defined terms External Connectivity, BES Cyber System and Routable External Connectivity** Drafting leads prepare for August Meeting with representatives from Industry stakeholder organizations
Washington, DC	7/28/2011	Drafting Team Meeting with FERC Staff
Atlanta, GA NERC	**8/16 - 8/18/2011**	**Review of Standards with Industry Representatives**
Interim Week 1	8/19 - 8/26/2011	Revise drafting requirements based on feedback from Industry Representatives
WEBINAR	**8/24/2011**	**Industry Webinar as outreach to present concepts and schedule for Version 5 CIP Standards**
Interim Week 2	8/25 - 9/2/2011	Revise drafting requirements based on feedback from Industry Representatives
LABOR DAY	9/5/2011	Labor Day Holiday
Interim Week 3	9/6 - 9/9/2011	Update rationale, change documentation and guidance to reflect requirements
Interim Week 4	9/12 - 9/16/2011	Review VRFs and VSLs modified from Version 4 Review CIP-010 and 011 informal comment/response document

Meeting Location	Dates	Meeting Objective
Westminster, CA SCE	**9/20 - 9/22/2011**	**CSO706 Drafting Team approves CIP Standards, implementation plan, and other documentation for NERC Quality Review (QR)**
Quality Review Prep	9/23/2011	Finalize and Issue Version 5 Documents for NERC Quality Review
NERC Quality Review	9/26 - 10/14/2011	NERC Quality Review & meeting with DT leadership and subteam leads to provide comments
Interim	10/17 - 10/24/2011	Subteams to review and update standards and all documentation based on QR and prepare for posting
Constellation Baltimore, MD	**10/25 -10/27/2011**	**SDT Meeting to consider QR changes made to the standards and finalize standards for posting**
Interim	10/28 - 11/2/2011	SDT Finalizes CIP V5 Documents for Posting
POSTING	11/3/2011	Post CIP Standards for 45^{+} day formal comment with concurrent ballot
Comment & Ballot Period	11/4 - 12/19/2011	Version 5 CIP Standards 45^{+} day formal Comment and Ballot Period
	11/4 - 11/14/2011	SDT Members Prepare for Industry Webinar on CIP V5 Standards
WEBINAR	**11/15/2011**	**Industry Webinar as outreach to present concepts and schedule for Version 5 CIP-002 standard requirements, the overall format of the standards, the definitions used and the implementation plan.**
	11/16 - 11/28/2011	SDT Members Prepare for Industry Webinar on CIP V5 Standards
WEBINAR	**11/29/2011**	**Industry Webinar as outreach to present concepts and schedule for Version 5 CIP-003 through CIP-011 Standards**
Web Conference	**11/30 - 12/1/2011**	**Drafting Team Meeting to review Webinar questions and comments**
	12/20 - 12/21/ 2011	NERC Staff Prepares Industry Comments and Ballot Comments Received for Review by SDT

Meeting Location	Dates	Meeting Objective
Review Comments	12/22/2011 - 1/23/2012	Review formal comments and concurrent ballot comments. NERC will prepare initial draft responses to comments for SDT consideration. SDT to begin update of standards text based on feedback received through industry comments and ballot comments.
FRCC (Tampa, FL)	**1/24 - 1/26/2012**	**Drafting Team Meeting to review initial responses to comments, prepare additional responses to formal comments and ballot comments, and continue to update text of standards**
Interim	1/27 - 2/10/2012	Drafting Team prepares updates to the CIP standards text based on feedback from 45-day comment and ballot period
Interim	2/13 - 2/20/2012	Continue to review industry comments and incorporate changes into the text of the standards Revise standards for re-posting for 30-day comment and ballot period
APS (Phoenix, AZ)	**2/21 - 2/23/2012**	**Drafting Team Meeting to finalize & approve responses to formal comments and finalize standards documents for Quality Review.** **SDT to prepare documents for NERC QR**
NERC Quality Review	2/24 –3/19/2012	NERC Quality Review of Responses to Industry Comments from 45-day comment & ballot period. Quality Review of related updates to the CIP standards
Interim	3/12 - 3/19/2012	SDT updates standards and all documentation based on QR and prepares for posting for 30-day comment & ballot period
WEB Conference	**3/20 - 3/21/2012**	**SDT Meeting to consider QR changes made to the standards and finalize standards for 30-day formal comments and successive ballot posting**
Interim	3/22 - 3/23/2012	NERC Prepares Documents for Successive Ballot

Meeting Location	Dates	Meeting Objective
POST Responses to Comments	3/26/2012	Post responses to 45-day formal comments with concurrent ballot comments
Comment & Ballot	3/26 - 4/27/2012	30-day Posting of CIP Standards for comments with successive ballot
Interim	3/26 - 4/25/2012	Begin preparation of FERC filing documentation
Interim	4/30 - 5/1/2012	NERC Staff Prepares Industry Comments and Ballot Comments Received for Review by SDT
Interim	5/2 - 5/22/2012	Subteam meetings to prepare responses to successive ballot comments and revise text of CIP Standards, as necessary
Location (??)	**5/22 - 5/24/2012**	**Drafting Team Meeting to finalize responses to comments and prepare revisions to CIP Standards for recirculation ballot (10-days)**
NERC Quality Review	5/25 - 6/8/2012	NERC Quality Review of Responses to Industry Comments from 30-day comment & ballot period Quality Review of related updates to the CIP standards
Post for Ballot	6/11/2012	Post for recirculation ballot
Interim	6/11- 6/22/2012	Recirculation Ballot
Finalize Standards	6/25 - 6/29/2012	Finalize CIP standards text for approval by NERC BOT

Appendix 5: Project 2008-06 CSO 706 Needs, Goals, and Objectives

NEED, GOALS AND OBJECTIVES – PROJECT 2008-06 - CIP CYBER SECURITY STANDARDS V5 – ADOPTED JANUARY 2011

NEED

The need for Critical Infrastructure Protection (CIP) in North America has never been more compelling or necessary than it is today. This is especially true of the electricity sector. Electric power is foundational to our social and economic fabric, acknowledged as one of the most essential and among the most targeted of all the interrelated critical infrastructure sectors.

The Bulk Electric System (BES) is a complex, interconnected collection of facilities that increasingly uses standard cyber technology to perform multiple functions essential to grid reliability. These BES Cyber Systems provide operational efficiency, intercommunications and control capability. They also represent an increased risk to reliability if not equipped with proper security controls to decrease vulnerabilities and minimize the impact of malicious cyber activity.

Cyber attacks on critical infrastructure are becoming more frequent and more sophisticated. Stuxnet is a prime example of an exploit with the potential to seriously degrade and disrupt the BES with highly malicious code introduced via a common USB interface. Other types of attacks are network or Internet-based, requiring no physical presence and potentially affecting multiple facilities simultaneously. It is clear that attack vectors are plentiful, but many exploits are preventable. The common factors in these exploits are vulnerabilities in BES Cyber Systems. The common remedy is to mitigate those vulnerabilities through application of readily available cyber security measures, which include prevention, detection, response and recovery.

In the cyber world, security is truly only as good as its weakest implementation. The need to identify BES Cyber Systems and then protect them through effective cyber security measures are critical steps in helping ensure the reliability of the BES functions they perform.

In approving Version 1 of CIP Standards CIP-002-1 through CIP-009-1, FERC issued a number of directives to the ERO. Versions 2, 3 and 4 addressed the short term standards-related and Critical Asset identification issues from these directives. There are still a number of unresolved standards-related issues in the FERC directives that must be addressed. This version is needed to address these remaining directives in FERC Order 706.

GOALS AND OBJECTIVES

- **Goal 1:** To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.
    - **Objective 1.** Provide a list of each directive with a description and rationale of how each has been addressed.
    - **Objective 2.** Provide a list of approved interpretations to existing requirements with a description of how each has been addressed.
    - **Objective 3.** Provide a list of CAN topics with a description of how each has been addressed.
    - **Objective 4.** Consider established security practices (e.g. DHS, NIST) when developing requirements.
    - **Objective 5.** Incorporate the work of Project 2010-15 Urgent Action SAR.
- **Goal 2:** To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.
    - **Objective 6**: Transition from a Critical Cyber Asset framework to a BES Cyber System framework.
    - **Objective 7.** Develop criteria to identify and categorize BES Cyber Systems, leveraging industry approved bright-line criteria in CIP-002-4.
    - **Objective 8.** Develop appropriate cyber security requirements based on categorization of BES Cyber Systems.
    - **Objective 9.** Minimize writing requirements at the device specific level, where appropriate.
- **Goal 3:** To provide guidance and context for each Standard Requirement
    - **Objective 10.** Use the Results-Based Standards format to provide rationale statements and guidance for all of the Requirements.
    - **Objective 11.** Develop measures that describe specific examples that may be used to provide acceptable evidence to meet each requirement. These examples are not all inclusive ways to provide evidence of compliance, but provide assurance that they can be used by entities to show compliance.
    - **Objective 12.** Work with NERC and regional compliance and enforcement personnel to review and refine measures.
- **Goal 4:** To leverage current stakeholder investments used for complying with existing CIP requirements.

  - **Objective 13.** Map each new requirement to the requirement(s) in the prior version from which the new requirement was derived.
  - **Objective 14.** Justify change in each requirement which differs from the prior version.
  - **Objective 15.** Minimize changes to requirements which do not address a directive, interpretation, broad industry feedback or do not significantly improve the Standards.
  - **Objective 16.** Justify any other changes (e.g. removals, format)

- **Goal 5:** To minimize technical feasibility exceptions.
  - **Objective 17.** Develop requirements at a level that does not assume the use of specific technologies.
  - **Objective 18.** Allow for technical requirements to be applied more appropriately to specific operating environments (i.e. Control Centers, Generation Facilities, and Transmission Facilities). (also maps to Goal 2)
  - **Objective 19.** Allow for technical requirements to be applied more appropriately based on connectivity characteristics. (also maps to Goal 2)
  - **Objective 20.** Ensure that the words "where technically feasible" exist in appropriate requirements.
- **Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to compliment a "culture of compliance".
  - **Objective 21.** Work with NERC Compliance Staff to evaluate options to reduce compliance impacts such as continuous improvement processes, performance based compliance processes, or SOX-like evaluation methods.
  - **Objective 22.** Write each requirement with the end result in mind, (minimizing the use of inclusive phrases such as "every device," "all devices," etc.)
  - **Objective 23.** Minimize compliance impacts due to zero-defect requirements.
- **Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
  - **Objective 24.** Avoid per device, per requirement compliance dates**.**
  - **Objective 25.** Address complexities of having multiple versions of the CIP standards in rapid succession.
  - **Objective 26.** Consider implementation issues by setting realistic timeframes for compliance.
  - **Objective 27.** Rename and modify IPFNICCAANRE to address BES Cyber System framework.

Appendix 6: Questions for FERC Technical Staff on NERC CIP V5 Working Draft

1. In its development of CIP-002-5, the SDT used a 3 tier categorization for the application of controls based on impact of BES Cyber Systems to the BES: large control centers (e.g., RC, BA, TOP) for High Impact, significant impact field transmission and generation assets and other control centers for Medium Impact, and remaining field assets for Low Impact. This approach is based on criteria developed in Version 4, currently filed for consideration by FERC. The SDT seeks FERC technical staff's comment on the approach to categorization of BES Cyber Systems and BES Cyber Assets.
2. The SDT removed the exception for cyber assets that do not use routable protocols that was included in previous versions of CIP-002. The SDT has addressed differences due to connectivity type as an applicability issue, where warranted, on a per requirement basis. The SDT seeks FERC technical staff's opinion on whether this adequately addresses the connectivity issue raised in previous versions.
3. In CIP-003-5, the SDT has removed requirements relating to exceptions to entities' security policies since it considers this a general management issue that is not within the scope of a compliance requirement. This is considered to be an internal policy requirement and not a reliability requirement. The SDT seeks FERC staff's comment on this approach.
4. The FERC Order directed the drafting team to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The drafting team has attempted to address this directive by requiring a framework for the configuration management process that includes a documented baseline configuration, explicit authorization for changes, and configuration monitoring for High Impact BES Cyber Systems. The SDT seeks FERC technical staff's comment on this approach.
5. In CIP-004-5, in the revocation of access section, the SDT has specified ***immediate revocation of the ability to access*** cyber systems for terminated personnel or personnel no longer requiring access to cyber systems. The SDT seeks FERC's comments on this issue.
6. In CIP-005-5, the SDT has included a requirement for detecting intrusions or malicious communication (IDS) in addition to access control and monitoring of the electronic access points in response to FERC's comments on defense in depth. The SDT seeks FERC technical staff's comment on the SDT's approach.
7. In CIP-006-5, the SDT has included a requirement for at least two "different and complementary" physical access control measures for the physical security boundary in

response to FERC's comments on defense in depth. The SDT seeks FERC technical staff's comment on the SDT's approach.

8. The SDT has included process improvement features in CIP-004-5 R6 and CIP-007-5 R4 that addresses the problem of zero defect in current corresponding requirements. The SDT requests FERC technical staff's comments on this approach.
9. The SDT has used "to the maximum capability of a device" in seven requirements. The SDT has used this approach to avoid drafting to the lowest common denominator, while providing the most appropriate level of the cyber security control in the requirement. The use of this phrase requires the entity to use the maximum capability of the BES Cyber Asset or BES Cyber System to meet the requirement in instances where device limitations otherwise preclude meeting the thresholds. The SDT believes that this provides, where appropriate, the necessary oversight through the requirements language for legacy devices and the existing audit process, without the need for the additional overhead of a Technical Feasibility Exception. The SDT requests FERC technical staff's comments on this approach.

Appendix 7: Meeting Evaluation Summary – Raw Data

Question 1

How would you rate the overall meeting in accomplishing the necessary objectives?

Average **3.2 / 4** **Last Month** **3.6/4**

Comments Audio levels were too low for most of the speakers

Question 2

How would you rate the effectiveness of the chair/vice chair?

Average **3.2 / 4** **Last Month** **3.6/4**

Comments Chair continues to inappropriately interrupt out of turn and forget to use his microphone. Vice chair very good at interceding when appropriate & necessary to facilitate meeting.

Excellent

Question 3

How would you rate the effectiveness of distributed agenda and meeting materials prior to this meeting?

Average **3.5 / 4** **Last Month** **3.8/4**

Comments Did not receive current full set of materials or know where to access for download. Also something weird on NERC registration site & available info immediately upon registration vs. 2 days prior to travel.

Agenda was not sent out to the plus list or made available when registering for the meeting.

Question 4

How would you rate the use of visual and audio aides for this meeting?

Average **3.0 / 4** **Last Month** **2.7/4**

Comments font size still an issue

Could not hear some of the speakers

Question 5

How would you rate the use of sub-team meetings in between face-to-face meetings?

Average 2**.7 / 4** **Last Month** **2.2/4**

Comments being revisited, but seems way to sneak stuff in past full team

Question 6

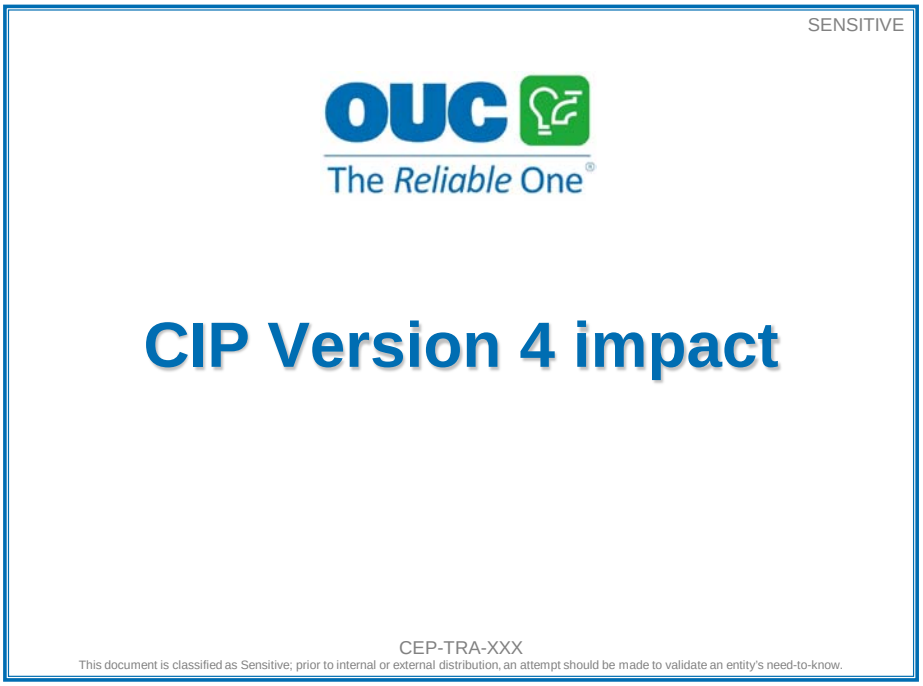
Please provide other suggested improvements or any other general comments.

Comments Subteam tweaks appear appropriate, so looks on track

Seeing the diagrams would have helped me follow the discussion. I missed some of the discussion because I'm in a different time zone. Thanks for allowing me to listen in.

Make the security code available when you register for the meeting. Observers who are following via phone while not viewing the ReadyTalk do not have access to the security code.

Appendix 8: CIP Version 4 Impact



The full presentation is attached in a separate presentation file.

Appendix 9: Sample Transmission Substation Information

Three PDF Files are attached to these minutes that represent the Transmission Substation Example information that was examined by the CSO706 Drafting Team when reviewing the Version 5 Draft Cyber Security Standards during this meeting.

These files are:

a. CIP v5 Exercise - Inventory.pdf
b. CIP v5 Exercise - Requirement Comments.pdf
c. CIP v5 Exercise - Substation Diagrams.pdf

Appendix 10: Sample Transmission Substation Information

Two PDF Files are attached to these notes that represent the Generation Station Example information that was examined by the CSO706 Drafting Team when reviewing the Version 5 Draft Cyber Security Standards during this meeting.

These files are:

a. CIP v5 Gen Example Process.pdf
b. CIP v5 Gen Example Requirements Comments.pdf