NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706
34th Meeting Summary

Little Rock, AR

Tuesday, May 17, 2011 |8 a.m. to 6 p.m. CDT
Wednesday, May 18, 2011|8 a.m. to 6 p.m. CDT
Thursday, May 19, 2011|8 a.m. to 6 p.m. CDT

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

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

Cyber Security Order 706 SDT- Project 2008-06
34TH MEETING
May 17-19, 2011
Little Rock, AR

Executive Summary

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to the Little Rock Meeting of the CSO706 SDT, and thanked them for their participation in this meeting. John also acknowledged Phil Huff, the meeting host and Vice-Chair, and his Arkansas Electric Cooperative Corporation (AECC) Team for all of their efforts in making this meeting possible. Phil reviewed the meeting location logistics and expressed his thanks to his support team and corporate management in helping to organize the meeting. Joe Bucciero, NERC Facilitator, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each meeting day. On Tuesday morning, the SDT unanimously adopted without comment the April 12-14, 2011, Sacramento, CA meeting summary.

The chair outlined the objectives the SDT sought to accomplish by the end of this meeting that included team review of CIP Version 5 multiple standard format, review and refinement of CIP V5 BES Cyber System identification and security requirements, review and finalize the style guide for drafting the CIP requirements, review the initial drafts of the CIP-002 through CIP-011 requirements, review of the implementation plan concepts, and agreement on the team's next steps and assignments. **Appendix 1** contains the meeting agenda packet.

The Chair reported that team still desires another Canadian representative, which is posted as a vacancy for the team. He also announced that Jon Van Boxtel has resigned his post at Portland General and his continued participation on the Standard Drafting Team is doubtful. **Appendix 2** contains the meeting attendance list, and the current drafting team roster is included as **Appendix 3**.

Industry Review:

Scott Mix and John Lim provided an update on other industry activity regarding cyber security. They reported on the NERC Cyber Security Task Force meetings, and the discussions and plans of the DOE led Risk Management Program. The target is to have a first draft report from the Risk Management Program (RMP) group by the end of May 2011. The connection with the CIP standards is currently very minor, as the group has been focused on developing a risk management process based approach for cyber security that is much broader in scope than the CIP standards. They are looking at end-to-end cyber security.

Scott reported on the progress of the updates to CIP-005-4 regarding remote access. He reported that the revised CIP-005 comments and ballot period closed on April 28, 2011. The industry approval rating for the CIP-005-4 document dropped from about 42% to 38% in the last ballot. Among the major issues were: the possible impact on transmission operations; the potential for contract re-negotiations with existing system vendors; the unavailability of standard contract language that can be adopted and used by the industry; the difficulty to audit and enforce the requirements at the vendor locations and at the potential remote locations used for maintenance by utility personnel; and the potential double jeopardy issues that existed. Scott indicated that a call was held with the Standards Committee on May 13, and the Urgent Action Team recommended that it be disbanded and that the requirements be picked-up by the CSO706 SDT for resolution and incorporation into the Version 5 CIP Standards on Cyber Security. The SC asked to hear an official response from the CSO706 SDT leadership that the SDT will assume the role of incorporating the remote access requirements into the CSO706 standards. The CSO706 SDT voted and agreed to assume this role.

John Lim reported that the group of EEI Member Company representatives who are members of the CSO706 SDT met with the EEI members to give them a preview of the requirements included in Version 5 of the CIP Standards on cyber security. In addition to John Lim, the CSO706 SDT Members included Jay Cribb, Jerry Freese, Doug Johnson, Scott Rosenberger, Tom Stevenson, and Bill Winters. They believe that EEI provided them with a generally positive response on the approach to the development of the Version 5 CIP standards on Cyber Security, and that the thinking of some members was positively influenced by what they heard from the SDT Members present.

Jim Brenton (ERCOT) reported on the progress being made on the DOE Security Roadmap. Jim provided the following summary for the minutes:

> *"The Cross-Sector Roadmap to Secure Control Systems describes a plan for voluntarily improving cyber security across all critical infrastructure/key resources (CIKR) that employ industrial control systems. This roadmap will provide an opportunity for industry experts to offer input concerning the state of control systems cyber security and to communicate recommended strategies for improvement. This roadmap brings together various sector stakeholders, government agencies, and asset owners and operators, with a common set of goals and objectives. It also provides milestones to focus specific efforts and activities for achieving the goals and addressing control system's most urgent challenges, longer-term needs, and practices for improvement."*

Jim also provided a copy of the DOE Roadmap to Secure Energy Delivery Systems, a hotlink to which is included in **Appendix 8**.

Scott also reported that NERC is forming a CIP Interpretations Drafting Team that will help organize and respond to all of the CIP Interpretations, and that team will have its own assigned NERC Coordinator.

Drafting Team Schedule

Phil Huff and Joe Bucciero reviewed the current project and meeting schedule (See **Appendix 4**) with the drafting team, and the team discussed possible meeting dates, objectives, and locations. The SDT is targeting the June 2011 meeting to have an open session with representatives from the Regional Audit/Compliance teams in Springfield, MO at AECI's facilities to review an early draft of the Version 5 CIP Cyber Security Standards, but primarily to receive some feedback on the concerns and issues that have been existing with the Version 3 standards, and the anticipated issues with the Versions 4 and 5 CIP Cyber Security standards. The drafting team is also planning to hold a full-day meeting with FERC's technical staff in Washington, DC to obtain their thoughts and insights into the Version 5 Reliability Standards on Cyber Security. The SDT is also targeting the August 2011 meeting to meet with representatives from the industry stakeholder organizations at NERC's Offices in Atlanta to discuss (in workshop fashion) the requirements of the Version 5 CIP standards.

Joe Bucciero will prepare a draft updated project schedule for the team to review at the next CSO706 SDT meeting in Springfield, MO.

Subteam Assignments

The current makeup of each sub-team is provided in **Appendix 5** for reference.

Needs, Goals, & Objectives

The drafting team was reminded of the Needs, Goals, and Objectives it previously developed. (**Appendix 6**)

Style Guide

The Style Guide for the standards is included as **Appendix 7.**

Format of CIP Version 5 Standards & Framework

The SDT reviewed the CIP-002-5 draft requirements. It was decided that a 'definitions' document was needed that would include all of the 'local' definitions in one place and remove them from the individual standards. While this may be OK for the drafting process, clarification is needed to determine if the definitions can remain as a separate document or must they be incorporated into the individual standard documents during the balloting process.
Joe Bucciero will check with Maureen and Laura to get a determination.

The relationship between each of the operational functions identified in CIP-002 and the NERC Functional Model was discussed. The drafting team is trying to determine if relating the operational functions with each item in the Functional Model would provide any additional clarity vs. defining the operational functions separately in the standards. The drafting team also discussed the possibility of identifying the "Low Impact" BES Systems and functions, and including this information upfront in CIP-002-5.

John Lim will review the mapping of the operational functions to the Functional Model.

Requirement R1 of CIP-002-5 was also discussed, and in particular the statement in 1.1 that requires the following updates and update period:

> *"Update the identification and categorization within 45 calendar days of the completion of a planned change to the BES or to the BES Cyber Assets or BES Cyber System."*

The drafting team considered three options:

1. Leave wording as is currently stated
2. Change the update period to 30 days and make it only applicable to BES changes
3. Remove the item 1.1 entirely

The discussions centered on the update period (45-days) as well as the extent of the applicability of the requirement (High/Medium/Low Impact systems).

The results of the discussion were that we would leave the words as they are for now, but discuss them at the June 2011 meeting with the regional audit/compliance staff representatives.

Other issues that were raised focused on the criteria list as stated in Attachment 1, Impact Categorization of BES Cyber Assets and BES Cyber Systems. Among the items mentioned were:

(a) The 300MW load level threshold stated in Criterion 2.13 is too low
(b) The Low to Medium Impact thresholds need to be re-evaluated (may be too high)
(c) AEP provided threshold cross-reference document (**Appendix 9**) needs further review

John Lim and the CIP-002-5 drafting subteam will consider these items as they meet over the next month, and report back to the SDT at the July 2011 meeting.

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. Each of the teams will continue to meet over the next week and finalize their respective draft requirements. The drafts of the CIP-002 through CIP-011 standards will be sent to the regional audit/ compliance representatives by the end of next week.

1. CIP-003 Report:
    a. Biggest change reported in CIP-003 is the removal of the "table format" for the standard requirements. All entities must comply with all of the CIP-003 requirements.
    b. The subteam needs to further review the specificity of the "delegation of responsibility" of the senior manager as stated in R5 of the standard.
2. CIP-004 Report:
    a. Subteam will review the periodicity required for the availability of security practices
    b. Subteam will clarify to whom the security practices should be available.
    c. Role-based training vs. appropriate training needs further clarification (e.g., is some training required on every topic to all role-based groups; what are the different levels of training based on the role of the individuals being trained?)
    d. The content of R2 and R3 needs review regarding paragraph references to Order 706, coordination with EOP-004 regarding the definition of a cyber security incident; the applicability of Item 3.1 to All REs (vs. High/Medium Impact BES Systems).
    e. Item 4.8: Personal Risk Assessment (PRA) vs. ID Verification – what is required when. Is an ID Verification check required with each PRA every 7 years?
    f. Item 4.7: Is a PRA required for access to Low Impact BES Cyber Systems?

The SDT was polled regarding the removal of the requirement text that specifies the details to be included in a PRA every 7 years: 12 agreed to remove the details; 3 did not agree.

The drafting sub-team will review if security practice awareness material needs to be made available to personnel who have electronic access or unescorted physical access to the BES Cyber Systems, and that this material is updated on a quarterly basis.

The drafting subteam will review and consider the suggested changes to the requirements in its meetings next week.

3. CIP-006 Report:
    a. Discussions centered on the physical access control requirements and the electronic access control requirements. For Low Impact BES Cyber Systems, are physical access controls required or can electronic access controls do the job and meet the needs?
    b. Electronic boundary for Low Impact BES Cyber Systems – how will this be measured? Does the measure always need to be documentation? Can it be a site visit? FERC's oversight role would likely require that something be done for the Low Impact BES Cyber Systems – a programmatic only solution may not be enough.
    c. It was recognized that individually, the Low Impact BES Cyber Systems may not be an issue, but in concert they could represent a more significant impact.
    d. Coordination with the regional audit/compliance teams and review of NIST 800-53A may be helpful to determine the best way to measure compliance with the requirements for Low Impact BES Cyber Systems without requiring lots of documentation. Possibly, a 'sampling' can be done vs. 'spot-checking' to determine compliance.
    e. Subteam will consider combining Items 1.1 and 1.2 and coordinating with requirements in CIP-004.
    f. Should BES Cyber Systems without connectivity be considered as Low Impact?
    g. Should Medium Impact BES Cyber Systems without external connectivity be considered as Low Impact?
    h. Should multi-entry (and exit) capability be available on a daily access basis? Check with NIST 800-53.

The drafting team was polled regarding the continued use of operational and procedural controls for Low Impact BES Cyber Systems – specifically with respect to physical access security: 12 agreed to continue with operational and procedural controls; 2 did not agree.

4. Other CIP Standards were considered without comment at this time. Drafting subteams will continue to work on any outstanding issues.

Action Items

Some of the action items taken from the subteam discussions are as follows:

Joe Bucciero will check with Maureen regarding the numbering of the revision to the standards for CIP-010 and CIP-011. Can these standards be labeled as CIP-010-5 and CIP-011-5, or do we need to start with CIP-010-1 and CIP-011-1?
Joe reported that NERC advised that the new CIP-010 and CIP-011 standards must begin with Version 1 (not Version 5, as CIP-002 through CIP-009 will be designated).

The drafting team leadership indicated that it will take up this item with NERC and the Standards Committee. The drafting team wants to use Version 5 for all of the latest CIP Standards (CIP0002 through CIP-011).

How can the need for training related to the "low impact" assets be incorporated into the training requirements?

The Access Control subteam will review and revise the requirements for password length and periodicity of update with respect to applicable devices.

Do we need to be concerned about wireless technologies such as microwave, optical fiber, radio, cellular, etc.?

When reviewing items of a requirement, do self-determined violations of the standard require a self-report? How is this situation handled in existing standards – like vegetation management?

Subteam Meeting Schedules & Full SDT Discussions

Each of the subteams scheduled their respective meetings between now and the Springfield, MO meeting in June 2011 to continue the development of their respective standards, and measures.

Phil Huff and John Lim agreed to lead the SDT in a dry run walkthrough of the CIP requirements at the July 2011 meeting (JULY 19-21) to prepare for the August Meeting with the Industry Stakeholder Group Representatives.

In preparation for the June 2011 (June 21-23) meeting with the Regional Audit staff representatives at AECI, a list of thoughts and 'to do' items were generated:

1. Provide the latest draft of the standards by June 3 for audit staff review prior to the meeting.
2. The discussions need to be time managed so that adequate time can be given to each standard
    a. Joe Bucciero will manage the time for the presenters and Q&A sessions
3. Extended "break" times should be included in the agenda to allow for additional discussion
4. The SDT should provide some context setting background prior to each discussion:
    a. Overview background – John Lim and Phil Huff
    b. Specific requirements – each subteam or subteam leads
5. Subteam leads should be the primary speakers, allowing for extended time for Q&A sessions

6. Consider an overview of the requirements by the subteam leads, and a Q&A panel of the subteam to respond to questions
7. Ask auditor staff to provide written feedback on problems with Version 3 and potential problems with Version 4 ahead of the meeting for further discussion
8. Ask auditors for feedback on the measures as included in the Version 3 and 4 standards

Scott and Phil will prepare a presentation slide deck ahead of the meeting.

Implementation Plan

A subteam was formed to draft the implementation plan for CIP Version 5 standards. Volunteers are welcome. Some of the challenges will be to keep the implementation plan fairly simple in light of the High, Medium, and Low impact levels being defined. A single date for all would likely mean a long time frame since there will be plenty of work to be done. We'll need to look for some quick hits that can be accomplished in the short term, while leaving some of the work to later. Some middle ground is needed to provide adequate time, but implementing the high impact items first.

Dave Revill agreed to provide a spreadsheet that would help describe what equipment is included in each of the 3 categories of impact (high, medium, and low). The FERC data request of NERC may help with this exercise.

Phil Huff and David Revill agreed to prepare the first cut strawman of the implementation plan requirements.

Adjournment

The Chair thanked everyone for attending the meeting, either in person or via the conference call facilities, and expressed his thanks to Phil Huff, Vice-Chair and Meeting Host, and his support team for their excellent job in hosting another meeting at AECC.

The meeting evaluation results are included as **Appendix 10**.

The meeting adjourned at 4:30 PM on Thursday, May 19, 2011

Appendix 1
Project 2008-06 Cyber Security Order 706 SDT
34th Meeting Agenda
May 17, 2011 Tuesday - 8:00 AM to 6:00 PM CDT
May 18, 2011 Wednesday - 8:00 AM to 6:00 PM CDT
May 19, 2011 Thursday - 8:00 AM to 5:00 PM CDT
Arkansas Electric Cooperative Corporation (AECC)
1 Cooperative Way, Little Rock, AR 72209

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review and refine CIP-002-5 through CIP-011-5 Requirements and Measures
- To review and discuss objectives and approach for June SDT meeting with NERC and Regional Compliance staff
- To review and discuss objectives and approach for walking through application of CIP Standards during July SDT meeting
- To review and discuss objectives and approach for August SDT meeting with industry trade associations
- To review and discuss communication plan
- To agree on next steps and assignments

Timed Agenda

Tuesday May 17, 2011 8:00 a.m. - 6:00 p.m. CDT

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

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

8:20 **Industry Review**- *Scott Mix, NERC, Mike Keane, FERC and others*
- FERC Information request
- DOE/NIST/NERC Risk Management Process
- CIP-005-4 Update
- EEI Meeting with EEI SDT members
- Other Cyber Security business

8:30 **Review Project Schedule –** *Philip Huff/Joe Bucciero*

8:50 **Review of CIP 002-5 Definitions**– *John Lim*

10:00 *Break*

10:15 **Review of CIP 002-5 Definitions (Cont'd) –** *John Lim*

12:00 *Lunch*

1:00 **Review of CIP-002-5 Requirements, Measures and Appendix –** *John Lim*

3:00 *Break*

3:15 **Review of CIP-003-5 – Security Management Controls (2) -** *Dave Revill*

4:30 **Review of CIP-004-5 – Personnel Security Controls (2) –** *Doug Johnson*

5:50 **Review any Drafting Assignments and Wednesday's Agenda**

6:00 *Recess*

Appendix 1
Project 2008-06 Cyber Security Order 706 SDT
34th Meeting Agenda
May 17, 2011 Tuesday - 8:00 AM to 6:00 PM CDT
May 18, 2011 Wednesday - 8:00 AM to 6:00 PM CDT
May 19, 2011 Thursday - 8:00 AM to 5:00 PM CDT
Arkansas Electric Cooperative Corporation (AECC)
1 Cooperative Way, Little Rock, AR 72209

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review and refine CIP-002-5 through CIP-011-5 Requirements and Measures
- To review and discuss objectives and approach for June SDT meeting with NERC and Regional Compliance staff
- To review and discuss objectives and approach for walking through application of CIP Standards during July SDT meeting
- To review and discuss objectives and approach for August SDT meeting with industry trade associations
- To review and discuss communication plan
- To agree on next steps and assignments

Wednesday May 18, 2011 8:00 a.m. - 6:00 p.m. CDT

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Joe Bucciero*
8:15	**Review and Refine CIP-004-5 – Personnel and Training (2) –** *Philip Huff and Roger Fradenburgh*
9:30	**Review and Refine CIP-005-5 – ESP (2) –** *Jay Cribb*
10:00	*Break*
10:30	**Review and Refine CIP-005-5 – ESP (2) (cont'd) –** *Jay Cribb*
11:30	**Review and Refine CIP-006-5 – Physical Security (2) –** *Doug Johnson*
12:30	*Lunch*
1:30	**Review and Refine CIP-007-5 – System Security (6) –** *Jay Cribb*
3:00	*Break*
3:15	**Review and Refine CIP-007-5 – System Security (6) (cont'd) –** *Jay Cribb*
5:50	**Review any Drafting Assignments and Thursday's agenda**
6:00	*Recess*

Appendix 1
Project 2008-06 Cyber Security Order 706 SDT
34th Meeting Agenda
May 17, 2011 Tuesday - 8:00 AM to 6:00 PM CDT
May 18, 2011 Wednesday - 8:00 AM to 6:00 PM CDT
May 19, 2011 Thursday - 8:00 AM to 5:00 PM CDT
Arkansas Electric Cooperative Corporation (AECC)
1 Cooperative Way, Little Rock, AR 72209

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review and refine CIP-002-5 through CIP-011-5 Requirements and Measures
- To review and discuss objectives and approach for June SDT meeting with NERC and Regional Compliance staff
- To review and discuss objectives and approach for walking through application of CIP Standards during July SDT meeting
- To review and discuss objectives and approach for August SDT meeting with industry trade associations
- To review and discuss communication plan
- To agree on next steps and assignments

Thursday May 19, 2011 8:00 a.m. - 5:00 p.m. CDT

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Joe Bucciero*
8:15	**Review and Refine CIP-008-5 and CIP-009-5 (6) – Incident Response Plan and Recovery Plan –** *Scott Rosenberger*
10:00	*Break*
10:15	**Review of CIP-010-5 (3) – Configuration Management and Vulnerability Assessments -** *Dave Revill*
11:00	**Review of CIP-011-5 (2) – Information Protection -** *Dave Revill*
12:00	*Lunch*
1:00	**Review and Discuss Objectives, Agenda and Approach for June Meeting with NERC and Regional Compliance Staff –** *John Lim/Phil Huff*
3:00	*Break*
3:15	**Discuss Implementation Plan Concepts–** *All*
3:45	**Review and Discuss Communication Plan–** *All*
4:15	**Discuss July/August Meeting Logistics –** *Joe Bucciero*
4:45	Review Action Items – *Joe Bucciero*
5:00	*Adjourn*

Appendix 1
Consensus Guidelines

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 2/3rds 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.

Appendix 1
Consensus Guidelines

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 Attendees List
May 17-19, 2011 (Little Rock, AR)

Name	Company	APR 12	APR-13	APR 14
1. Rob Antonishen	Ontario Power Generation	X	X	X
2. Jay Cribb	Southern Company Services	X	X	X
3. Joe Doetzl	Kansas City Power & Light	X	X	X
4. Gerry Freese	AEP	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. John Lim, Chair	Consolidated Edison Co. NY	X	X	X
8. Robert Preston Lloyd	Southern California Edison	X	X	X
9. David Revill	Georgia Transmission Corporation	X	X	X
10. Scott Rosenberger	Luminant Energy	X	X	X
11. Kevin Sherlin	Sacramento Municipal District	X	X	X
12. Tom Stevenson	Constellation	X	X	X
13. John D. Varnell	Tenaska Power Services Co.	X	X	X
Joe Bucciero	*NERC Facilitator*	*X*	*X*	*X*
Scott Mix	*NERCStaff*	*X*	*X*	*X*

Others Attending In Person or via ReadyTalk and Phone

Tom Alrich, Jan Bargen, Jim Brenton, John Carpenter, David Dockery, Jim Fletcher, David Gordon, Kuldeep Hak, Darren Highfill, Tom Hofstetter, Michael Keane, Drew Kittey, Brian Newell, Maggie Powell,

APPENDIX 3
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM ROSTER

CYBER SECURITY ORDER 706 STANDARD DRAFTING TEAM (PROJECT 2008-06)

1. Chairman	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
2. Vice Chairman	Philip Huff Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
3. Members	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@opg.com
4.	Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@southernco.com
5.	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@ duke-energy.com
6.	Gerald S. Freese Director, NERC CIP Compliance	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
7.	Christine Hasha Compliance Analyst Senior	Electric Reliability Council of Texas 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3909 (512) 248-3993 Fx christine.hasha@ ercot.com
8.	Jeffrey Hoffman Chief Architect, IT Policy and Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm 380 P.O. Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 jhoffman@usbr.gov
9.	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com
10.	Robert Preston Lloyd Sr. Technical Specialist, Substation Regulatory Compliance	SC&M Technical Support & Strategy Southern California Edison One Innovation Way Pomona, CA 91768	(626) 543-7863 (909) 274-1338 (626) 422-1346 M robert.lloyd@sce.com

APPENDIX 3
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM ROSTER

11.	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
12.	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@gatrans.com
13.	Scott Rosenberger Director, Security and Compliance	Luminant 500 North Akard Dallas, Texas 75201	(214) 812-2412 Scott.Rosenberger@ energyfutureholdings.com
14.	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
15.	Thomas Stevenson General Supervisor Engineering Projects	Constellation Energy 1005 Brandon Shores Rd Baltimore, MD 21226	(410) 787-5260 (410) 227-3728 Thomas.W.Stevenson@ constellation.com
16.	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 keith.stouffer@nist.gov
17.	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 jvarnell@tnsk.com
18.	William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@aps.com

APPENDIX 3
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM ROSTER

Consultant to NERC	Joseph Bucciero Standards Development Coordinator	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, PA 19525-9349	(267) 981-5445 joe.bucciero@gmail.com
NERC Staff	Tom Hofstetter Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax tom.hofstetter@nerc.net
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax roger.lampila@nerc.net
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 fax Scott.Mix@nerc.net

APPENDIX 4
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
SCHEDULE

CSO706 SDT
Meeting Schedule and Objectives (May 2011)

Development Process

- Face-to-face meetings used to review/refine the entire Standard. Full team reviews Standards to raise issues, formulate concepts to address issues, ensure consistency across sub-teams and further develop work products.
- Sub-teams meet in open web conferences in between face-to-face meetings to address issues raised by the full team.
- Full team 2 hour web conference the 2nd Thursday from 12:00a – 2:00p after every full team meeting to receive sub-team status updates and provide initial feedback.

Meeting Location	Dates	Meeting Objective
Columbus, OH AEP	01/18 to 01/20/2011	Develop Needs, Goals and Objectives. Develop project plan.
Interim	1/20 to 2/15/2011	Sub-Teams to: (1) develop/review rationale statements for each requirement in CIP-011, (2) document prior version references, and (3) develop change documentation for each table row.
Taylor, TX ERCOT	2/15 to 2/17/2011	Full review of Standards requirements, rationale and change justification Discussion with NERC Compliance staff on programmatic requirements
Interim	2/17 to 3/15/2011	Sub-teams continue drafting requirements.
New York, NY ConEd	3/15 to 3/17/2011	Document minimum level requirements, number of levels, degree of specificity, ensure consistent audibility and measurability Firm up communication plan, including outreach
Interim	3/17 to 4/12/2011	Sub-teams continue drafting requirements.
Sacramento, CA SMUD	4/12 to 4/14/2011	Review Mapping of Standards into CIP-002 to 00X Initial discussions on implementation plan.
Interim	4/14 to 5/17/2011	Sub-teams continue drafting requirements. Late April webinar on format, concepts

APPENDIX 4
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
SCHEDULE

Meeting Location	Dates	Meeting Objective
Little Rock, AR AECC	5/17 to 5/19/2011	Review of Standards and implementation plan
Interim	5/19 to 6/21/2010	Sub-teams continue drafting requirements.
Springfield, MO AECI	6/21 to 6/23/2011	Review of Standards with regional and NERC audit Staff
Interim	6/23 to 7/19/2011	Sub-teams continue drafting requirements based on feedback from regional and NERC audit staff.
Portland, OR (?) PGE	7/19 to 7/21/2011	Review of Standards and implementation plan based on feedback from regional audit staff
Interim	7/21 to 8/23/2011	Sub-teams continue drafting requirements based on review of audit staff feedback
Atlanta, GA NERC	8/16 to 8/18/2011	Technical workshop with invited industry representatives
Interim	8/19 to 9/19/2011	Sub-teams continue drafting requirements based on industry representative feedback
Pomona, CA SCE (?) or WECC	9/20 to 9/22/2011	SDT Meeting Quality assurance review with NERC staff to prepare standards for posting
Interim	10/5 to 11/20/2011	Posting for 45 day formal comment/ballot
	10/25/2011	Technical Webinar
Constellation Baltimore, MD	10/25 to 10/27/2011	SDT Meeting and Technical Webinar
Interim	11/17 to 12/13/2011	Continue responding to industry comments
FRCC	12/6 to 12/8/2011	Quality assurance review with NERC staff on posting for formal comment with concurrent ballot

Other options:
GTC
SERC
WECC

Appendix 5

CSO 706 SDT DRAFTING SUB-TEAMS
VERSION 5

Sub-Team	
CIP 002 **BES System Categorization**	John Lim (Lead), Rich Kinas, Robert Lloyd *(Observer Participants: Tom Sims, Jim Fletcher, Dave Dockery, Bryn Wilson, Martin Narendorf)* *(FERC: Mike Keane, Claudine Planter-Pascal)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Kevin Sherlin *(Observer Participants: Dave Dockery)* *(FERC: Drew Kittey, Matt Adeleke)*
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell, John Van Boxtel, Philip Huff, Christine Hasha *(Observer Participant: Brian Newell, Scott Raymond)* *(FERC: Justin Kelly, Matt Adeleke)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Ryan Breed)* *(FERC: Matt Adeleke, Claudine Planter-Pascal)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese, Robert Lloyd *(Observer Participants: Roger Fradenburgh, Martin Narendorf)* *(FERC: Mike Keane, Matt Dale)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly, Matthew Dale)*

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 7
Style Guide Considerations

General Omissions in Version 5 to Date

- **Guidance** – A few are almost complete. Several references for the need for additional guidance.
- **Summary of Changes** – Requirement level descriptions of change are largely inconsistent or missing. This includes how FERC directives are addressed, any requirements that were removed, and justification for major changes to requirements.
- **Non-BES Cyber Stuff –** This includes (1) Access Control systems (physical/electronic), (2) Electronic Access Points, (3) Monitoring systems, and (4) Non-Critical Cyber Assets within an ESP. Several ideas considered but nothing consistently documented.
- **Use of External Connectivity and Routable Protocols** – Rarely used as a scoping filter in requirements. Definitions have been proposed.
- **VRFs –** We can probably transfer a lot from version 3. Can we use impact levels?
- **VSLs –** We can probably transfer a lot from version 3.
- **Comment Response Summaries from CIP-011**
- **Implementation Plans**

IN ADDITION TO DRAFTING TECHNICALLY EXCELLENT REQUIREMENTS, THE SDT SHOULD FOCUS NEXT MONTH ON IMPROVING …

- NEED TO FOCUS ON DEFINING THE MEASURES IN PREPARATION FOR MEETING WITH THE AUDITORS
- NEED TO FOCUS ON NON-BES CYBER ITEMS ABOVE AS WELL AS VRF/VSLS
- EACH REQUIREMENT SHOULD HAVE A TIME HORIZON ASSOCIATED WITH IT (NEED SOME GUIDANCE ON THE APPLICABILITY OF THE TIME HORIZON REQUIREMENTS E.G., PLANNING, OPERATIONS PLANNING, REAL-TIME, ETC.)
-

Introductory Requirement

Style Guide Proposal:

Each Responsible Entity shall implement one or more processes that include the required items in CIP-011-1 [Table Title]

Ensure the consistent use of program, plan, process, and procedure. Programs contain plans. Plans consist of processes and procedures. The word "program" does not imply or infer any particular organizational structure.

Each responsible entity shall implement one or more documented (processes/plans/programs/policies) that include the required items in …

Examples:

CIP-003-5 R1	**R1.** Cyber Security Policy - Each Responsible Entity shall develop and implement one or more cyber security policies that include the required items in *CIP-003-5 Table R1 – Security Policy*.
CIP-004-5 R1	**R1.** Awareness - Each Responsible Entity with any BES Cyber Asset or BES Cyber System shall implement and maintain a security awareness program that includes the required items in *CIP-004-5 Table R1 – Security Awareness Program*.
CIP-005-5 R1	**R1.** Electronic Security Perimeter — Each Responsible Entity shall implement one or more processes that include the required items in *CIP-005-5 Table R1 – Electronic Security Perimeter*.
CIP-007-5 R5	**R1.** Each Responsible Entity shall implement, review, and maintain one or more processes for disabling unneeded ports and services that include the required items in CIP-007-5 Table R3 – Ports and Services
CIP-007-5 R5	**R1.** System Access Controls - Each Responsible Entity shall implement and document technical and/or procedural controls to control electronic access to BES Cyber Assets and BES Cyber Systems. Electronic access controls shall include the required elements in CIP-007-5 Table R5 – System Access Controls

Measures (START HERE __ 4/13/2011)

Style Guide Proposal

- *EACH MEASURE MUST IDENTIFY THE FUNCTIONAL ENTITY*
- *EACH MEASURE MUST BE TANGIBLE, PRACTICAL, AND AS OBJECTIVE AS IS PRACTICAL*
- *MEASURES SHOULD SUPPORT REQUIREMENTS BY IDENTIFYING WHAT EVIDENCE OR TYPES OF EVIDENCE COULD BE USED TO SHOW THAT AN ENTITY IS COMPLIANT WITH THE REQUIREMENT*
- *DO NOT USE "SHALL" OR "SHOULD" IN A MEASURE*

Examples

CIP-002-5 M1	The Responsible Entity shall have evidence identifying and documenting each of its BES Cyber Assets, and BES Cyber Systems and their constituent BES Cyber Assets, that executes or enables functions defined CIP-002 – 5 Attachment I – Functions Essential to the Reliable Operation of the BES as required in R1 and the functions it executes or enables.
CIP-003-5 M1	Verify that specific language in policy exists that address applicability to organizational and third-party personnel
CIP-004-5 M1	Perform a sample validation of the quarterly reinforcement material that has been distributed.
CIP-005-5 M1	Examples of acceptable evidence include a list for each BES Cyber System that names the Electronic Access Points for that system. If several BES Cyber Systems share the same EAPs, then one list for the group of systems is acceptable.

Applicability

Style Guide Proposal

- ***Impact Level*** – Specify either *Minimum* or *High Impact*. We may add a third impact level in the future, but these are the only choices at this time. Refer to Appendix A for additional guidance in determining the impact level. Only pertains to non-programmatic requirement types.
- ***Requirement Type*** – Specify All REs for programmatic requirements, BES Cyber System, or Component. Programmatic means the requirement applies only to having and implementing a program for all BES Cyber Systems but is not assessed at the system level. These are only candidate requirements at this time until we receive further guidance from NERC compliance staff. Component requirements indicate this requirement applies to individual components of the BES Cyber System.
- ***Operating Environment [Optional]*** – Specify *Control Center, Transmission Facility*, or *Generation Facility* if this requirement only applies to a specific operation environment. This means the BES Cyber System resides within that operating environment.
- ***External Connectivity Only [Optional]*** – Specify *External Connectivity Only* when the lack of connectivity provides compensating mitigation for a specific security requirement.

Examples

CIP-003-5 R1.1	All REs	**CIP-003-5 R3.1**	High
CIP-003-5 R4.1	High and Medium Impact, BES Cyber Systems	**CIP-003-5 R4.8**	High and Medium Impact, All REs
CIP-004-5 R4.1	All	**CIP-005-5 R1.2**	All BES Cyber Systems (which utilizes routable protocols)
CIP-006-5 R2.1	All Entities with High Impact BES Cyber Systems	**CIP-007-5 R4.2**	Medium Impact with external connectivity and High Impact BES Cyber Systems
CIP-008-5 R2.1	Plan(s) used to respond to Cyber Security incidents for Medium and High Impact BES Cyber Systems	**CIP-009-5 R1.1**	Plan(s) used to recover Medium and High Impact BES Cyber Systems

Rationale

Style Guide Proposal:

EACH REQUIREMENT MUST INCLUDE A RATIONALE SECTION. THE RATIONALE SECTION SHOULD STATE:

- WHY A REQUIREMENT IS NEEDED
- WHAT ASSUMPTIONS WERE MADE
- WHAT ANALYSIS EFFORT DROVE THE REQUIREMENT (IF NOT CONTAINED IN CIP VERSION 4)
- SOURCE OF ANY NUMBERS

Examples:

CIP-002-5 R1	BES Cyber Assets and BES Cyber Systems either directly execute or indirectly enable reliability functions necessary for the reliability and operability of the BES. In order to implement cyber security protective measures to ensure the availability, integrity and confidentiality of these assets and systems, it is necessary to identify them as a first step towards the implementation of these measures. Entities must identify discrete Cyber Assets that would be subject to these protective measures, or group them as BES Cyber Systems when a group of BES Cyber Assets together execute or enable one or more common reliability functions. In order to implement those measures that are applicable to discrete Cyber Assets, entities are required to also identify constituent BES Cyber Assets of BES Cyber Systems.
CIP-003-5 R1	One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements. The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs.
CIP-004-5 R1	Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices.
CIP-005-5 R1	The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.
CIP-006-5 R1	To control when personnel without authorized unescorted physical access can enter areas protecting physical access to High Impact BES Cyber Systems.
CIP-007-	The requirements set forth in Table R5 reflect generally-accepted good cyber

5 R5	security practices that are codified in many other security standards. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Using complex passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. Strong procedural and technical controls on the use of privileged accounts can help prevent systems from being taken over by attackers, and requiring privileged account users to log onto systems using their own, non-privileged accounts for non-administrative tasks supports accountability and reduces the risk of accidental misconfiguration.
CIP-008-5 R1	so that consistent responses to Cyber Security Incidents involving BES Cyber Systems can occur.

Appendix 8

DOE Roadmap to Secure Energy Delivery Systems

The latest DRAFT to the Roadmap to Secure Energy Delivery Systems provides an updated plan for the energy sector to further its efforts to improve the cyber security of energy delivery systems. This strategic framework presents the vision of industry, academia, and government stakeholders for energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next 10 years. It marks a continued effort by public and private stakeholders that identifies steps to build, deploy, and manage resilient energy delivery systems for the electric, oil, and natural gas industries.

This document is an update of the original 2006 Roadmap to Secure Control Systems in the Energy Sector that outlined the sector's ongoing commitment to security for control systems. North America's water, transportation, communication, and other critical infrastructures have a growing dependence on the reliable operation of the energy sector—making it an attractive target for increasingly sophisticated cyber adversaries. As cyber threats are fast moving, multifaceted, well resourced, and persistent, we need to ramp up efforts to effectively prepare and respond to them.

The link to the DOE website for this document is:

http://www.oe.energy.gov/DocumentsandMedia/2011_EDS_Roadmap_DRAFT_11111.pdf

Jim Brenton, CISSP-ISSAP

Regional Security Coordinator

ERCOT -- Principal

Appendix 9

CIP-002 Attachment 1 Comparison

Version 4 and Version 5

CIP-002-5 - Attachment I

IMPACT CATEGORIZATION OF BES CYBER ASSETS AND BES CYBER SYSTEMS

1. High Impact Rating (H)

Each BES Cyber Asset or BES Cyber System that can affect operations for:

1.1. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.14. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO PERFORM THE FUNCTIONAL OBLIGATIONS OF THE RELIABILITY COORDINATOR.

1.2. Each control center or backup control center used to perform the functional obligations of the Balancing Authority THAT INCLUDES AT LEAST ONE ASSET IDENTIFIED IN CRITERIA 1.1, 1.3, 1.4, OR 1.13. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO PERFORM THE FUNCTIONAL OBLIGATIONS OF THE BALANCING AUTHORITY for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

1.17. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO PERFORM THE FUNCTIONAL OBLIGATIONS OF THE BALANCING AUTHORITY THAT INCLUDES AT LEAST ONE ASSET IDENTIFIED IN CRITERIA 1.1, 1.3, 1.4, OR 1.13. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO PERFORM THE FUNCTIONAL OBLIGATIONS OF THE BALANCING AUTHORITY FOR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION.

1.3. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of one or more of the assets identified in criteria 2.2, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 or 2.12 below.

1.16. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO PERFORM THE FUNCTIONAL OBLIGATIONS OF THE TRANSMISSION OPERATOR THAT INCLUDES CONTROL OF AT LEAST ONE ASSET IDENTIFIED IN CRITERIA 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 OR 1.12.

1.4 Each control center or backup control center used to control generation AT MULTIPLE PLANT LOCATIONS, FOR ANY GENERATION FACILITY OR GROUP OF GENERATION FACILITIES IDENTIFIED IN CRITERIA 1.1, 1.3, OR 1.4. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED

TO CONTROL GENERATION equal to or exceeding 1500 MW in a single Interconnection.

1.15. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO CONTROL GENERATION AT MULTIPLE PLANT LOCATIONS, FOR ANY GENERATION FACILITY OR GROUP OF GENERATION FACILITIES IDENTIFIED IN CRITERIA 1.1, 1.3, OR 1.4. EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO CONTROL GENERATION EQUAL TO OR EXCEEDING 1500 MW IN A SINGLE INTERCONNECTION.

2. Medium Impact Rating (M)

Each BES Cyber Asset or BES Cyber System that can affect operations for:

2.1. EACH GROUP OF GENERATING UNITS (INCLUDING NUCLEAR GENERATION) AT A SINGLE PLANT LOCATION WITH An aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.1. EACH GROUP OF GENERATING UNITS (INCLUDING NUCLEAR GENERATION) AT A SINGLE PLANT LOCATION WITH AN AGGREGATE HIGHEST RATED NET REAL POWER CAPABILITY OF THE PRECEDING 12 MONTHS EQUAL TO OR EXCEEDING 1500 MW IN A SINGLE INTERCONNECTION.

2.2. EACH REACTIVE RESOURCE OR GROUP OF RESOURCES AT A SINGLE LOCATION (EXCLUDING GENERATION FACILITIES) HAVING An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities).

1.2. EACH REACTIVE RESOURCE OR GROUP OF RESOURCES AT A SINGLE LOCATION (EXCLUDING GENERATION FACILITIES) HAVING AGGREGATE NET REACTIVE POWER NAMEPLATE RATING OF 1000 MVAR OR GREATER.

2.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.3. EACH GENERATION FACILITY THAT THE PLANNING COORDINATOR OR TRANSMISSION PLANNER DESIGNATES AND INFORMS THE GENERATOR OWNER OR GENERATOR OPERATOR AS NECESSARY TO AVOID BES ADVERSE RELIABILITY IMPACTS IN THE LONG-TERM PLANNING HORIZON.

2.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.4. EACH BLACKSTART RESOURCE IDENTIFIED IN THE TRANSMISSION OPERATOR'S RESTORATION PLAN.

2.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource

- to the first interconnection point of the generation unit(s) to be started, or
- up to the point on the Cranking Path where two or more path options exist and including any single failure points in the cranking path to the first interconnection point of the generation unit(s) to be started, or
- up to the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started

as identified in the Transmission Operator's restoration plan.

1.5. THE FACILITIES COMPRISING THE CRANKING PATHS AND MEETING THE INITIAL SWITCHING REQUIREMENTS FROM THE BLACKSTART RESOURCE TO THE FIRST INTERCONNECTION POINT OF THE GENERATION UNIT(S) TO BE STARTED, OR UP TO THE POINT ON THE CRANKING PATH WHERE TWO OR MORE PATH OPTIONS EXIST, AS IDENTIFIED IN THE TRANSMISSION OPERATOR'S RESTORATION PLAN.

2.6.Transmission Facilities operated at 500 kV or higher.

1.6. TRANSMISSION FACILITIES OPERATED AT 500 KV OR HIGHER.

2.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.7. TRANSMISSION FACILITIES OPERATED AT 300 KV OR HIGHER AT STATIONS OR SUBSTATIONS INTERCONNECTED AT 300 KV OR HIGHER WITH THREE OR MORE OTHER TRANSMISSION STATIONS OR SUBSTATIONS.

2.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.8. TRANSMISSION FACILITIES AT A SINGLE STATION OR SUBSTATION LOCATION THAT ARE IDENTIFIED BY THE RELIABILITY COORDINATOR,

PLANNING AUTHORITY OR TRANSMISSION PLANNER AS CRITICAL TO THE DERIVATION OF INTERCONNECTION RELIABILITY OPERATING LIMITS (IROLS) AND THEIR ASSOCIATED CONTINGENCIES.

2.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. FLEXIBLE AC TRANSMISSION SYSTEMS (FACTS), AT A SINGLE STATION OR SUBSTATION LOCATION, THAT ARE IDENTIFIED BY THE RELIABILITY COORDINATOR, PLANNING AUTHORITY OR TRANSMISSION PLANNER AS CRITICAL TO THE DERIVATION OF INTERCONNECTION RELIABILITY OPERATING LIMITS (IROLS) AND THEIR ASSOCIATED CONTINGENCIES.

2.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

1.10. TRANSMISSION FACILITIES PROVIDING THE GENERATION INTERCONNECTION REQUIRED TO CONNECT GENERATOR OUTPUT TO THE TRANSMISSION SYSTEM THAT, IF DESTROYED, DEGRADED, MISUSED, OR OTHERWISE RENDERED UNAVAILABLE, WOULD RESULT IN THE LOSS OF THE ASSETS IDENTIFIED BY ANY GENERATOR OWNER AS A RESULT OF ITS APPLICATION OF ATTACHMENT 1, CRITERION 1.1 OR 1.3.

2.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.11. TRANSMISSION FACILITIES IDENTIFIED AS ESSENTIAL TO MEETING NUCLEAR PLANT INTERFACE REQUIREMENTS.

2.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.12. EACH SPECIAL PROTECTION SYSTEM (SPS), REMEDIAL ACTION SCHEME (RAS) OR AUTOMATED SWITCHING SYSTEM THAT OPERATES BES ELEMENTS THAT, IF DESTROYED, DEGRADED, MISUSED OR OTHERWISE RENDERED UNAVAILABLE, WOULD CAUSE ONE OR MORE

INTERCONNECTION RELIABILITY OPERATING LIMITS (IROLS) VIOLATIONS FOR FAILURE TO OPERATE AS DESIGNED.

2.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.13. EACH SYSTEM OR FACILITY THAT PERFORMS AUTOMATIC LOAD SHEDDING, WITHOUT HUMAN OPERATOR INITIATION, OF 300 MW OR MORE IMPLEMENTING UNDER VOLTAGE LOAD SHEDDING (UVLS) OR UNDER FREQUENCY LOAD SHEDDING (UFLS) AS REQUIRED BY THE REGIONAL LOAD SHEDDING PROGRAM.

2.14. Control Centers not included in High Impact Rating (H) above.

3. Low Impact Rating (L)

All other documented BES Cyber Assets and BES Cyber Systems that can affect operations and are not categorized in Section 1 as having a High Impact Rating (H) or Section 2 Medium Impact Rating (M).

Appendix 10
Meeting Evaluation Results
May 17-19, 2011

4 = Satisfied
3 = Generally Satisfied
2 = Somewhat Satisfied
1 = Dissatisfied

Question 1				
How would you rate the overall meeting in accomplishing the necessary objectives?				
	Average	3.3/4	**Last Month**	3.3/4
	Comments	should have been 4 days in order to cover all CIPs this time (20x20 hindsight) but advised when another big milestone is next month		
Question 2				
How would you rate the effectiveness of the full team in this meeting?				
	Average	3.2/4	**Last Month**	3.1/4
	Comments	get bogged down from time to time & lose focus		
Question 3				
How would you rate the effectiveness of the chair/vice chair?				
	Average	3.8/4	**Last Month**	3.6/4
	Comments	intervention seemed appropriate		
Question 4				
How would you rate the effectiveness of distributed agenda and meeting materials prior to this meeting?				
	Average	3.5/4	**Last Month**	3/4
	Comments	some presented mat'l still day-of but getting better		
Question 5				
How would you rate the use of visual and audio aides for this meeting?				
	Average	3.6/4	**Last Month**	3/4
	Comments	visual still sometimes small on screen		
Question 6				
How would you rate the use of sub-team meetings in between face-to-face meetings				
	Average	3.3/4	**Last Month**	3.3/4
	Comments	keep it up' but time-consuming		
Question 7				
Please provide other suggested improvements or any other general comments.				
	Comments			
		I didn't get the call-in info since there was no way to indicate on the signup that you were attending remotely. I'm told this will be changed for the next meeting.		
		Great location, good conversations, i thought it was very effective		
		At this stage, we could really benefit from a technical writer. We are struggling way too much with the language. We tend to have difficulty with grammar as well as documenting why we are making decisions. I would recommend this additional support from now until the completion of this project in June.		
		Excellent facilities		