NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706
35th Meeting Summary

Associated Electric Cooperative, Inc. (AECI)
Springfield, MO

Tuesday, June 21, 2011 |8 a.m. to 5 p.m. CDT
Wednesday, June 22, 2011|8 a.m. to 5 p.m. CDT
Thursday, June 23, 2011|8 a.m. to 5 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
35TH MEETING
June 21-23, 2011
Springfield, MO

Executive Summary

John Lim, chair of the CSO 706 SDT welcomed members and other participants to the Springfield, MO Meeting of the CSO706 SDT, and thanked them for their participation in this meeting. John also acknowledged Dave Dockery, the meeting host, and his Associated Electric Cooperative Incorporated (AECI) Team for all of their efforts in making this meeting possible. John also expressed his thanks to AECI's corporate management for their support to host and organize the meeting. John Bussman of AECI reviewed the meeting location logistics and expressed his thanks to his support team for all of their efforts.

Jim Jura, AECI's CEO, extended AECI's welcome to the drafting team and its guest participants and indicated that he considered it to be an honor and privilege to hold the drafting team meeting at AECI in Springfield, MO. Jim's welcoming remarks included his thanks for the open nature of work being done by the drafting team and in letting many interested parties contribute to the process of developing these cyber security standards for the various industry stakeholders. He also requested that the drafting team remain aware of the impact these standards could have on smaller companies in the Cooperative sector.

Joe Bucciero, NERC Facilitator, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each meeting day. On Wednesday morning, the SDT unanimously adopted the May 17-19, 2011, Little Rock, AR meeting summary. Joe also reviewed the meeting processes for the newcomers, and encouraged their participation. The meeting participants were reminded that the microphones in the meeting room were very sensitive and that the meeting was being recorded to ensure that the questions being raised were clearly understood and that accurate responses were being provided. There would be no transcription prepared from this meeting.

The chair welcomed the regional auditors to the meeting, expressed his appreciation for their time and effort to review and comment on the draft standards, and encouraged their input. The chair also outlined the objectives the SDT sought to accomplish by the end of this meeting, including the primary purpose of the meeting which was to review the auditor's issues and concerns with the currently approved version of the cyber security standards, as well as those potential concerns with the measurability and audit-ability of the draft Version 5 standards. As such, during the meeting the drafting team and the auditors reviewed the applicability and measurability of the requirements based on the current text of the draft standards, which had been sent to the auditors ahead of the meeting for their review and assessment. John Lim reminded everyone that the ReadyTalk conference call meeting was being recorded.

Appendix 1 contains the meeting agenda packet for this meeting.

The chair reported that the drafting team still desires another Canadian representative, which has been posted by NERC as a vacancy for the team. He also announced that Joe Doetzl has resigned his post at Kansas City Power & Light and his continued participation on the Standard Drafting Team is being discussed. **Appendix 2** contains the meeting attendance list, and the current drafting team roster is included as **Appendix 3**.

Industry Updates

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 NERC Cyber Security Task Force is reviewing various attack scenarios and has scheduled delivery of its report by the end of 2011.

Scott Mix reported on the status of the CIP 005-4 activities. The drafting team officially disbanded, and the work will be folded into the CSO706 team's work. The CSO706 team would have been involved once the CIP-005-4 work completed, in any event.

Howard Gugel reported that there has been an update on the FERC filing of the industry survey results (RM-11-11), and NERC is determining whether it needs to be a confidential filing

Overview of CIP Version 5

John Lim offered a presentation to the regional auditor teams about the current status of the standards development for CIP Version 5. **Appendix 8** contains a copy of this presentation.

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 (Steve Noess).

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. Following this June 2011 meeting with the Regional Audit/Compliance teams, 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.**

Overview of Issues and General Observations

Tom Hofstetter, NERC Staff, provided a brief presentation on the more significant issues being uncovered by the various audit teams concerning the CIP Standards. Some of these items are:

1. The organizational structure of the entities vs. compliance. The existing organizational structures seem to be requiring lots of input from different groups on the same items. The organizational structure has been having a more than expected impact on audit results.
2. Many companies are managing to compliance instead of managing their security. The $1M fine amount is easy to quantify for compliance, but the issues are really cyber security requirements.
3. CIP-006 R1.1 – six wall boundary – is the most violated standard requirement. This is a common problem that is also a recurring challenge.
4. Blackstart requirements are also a recurring challenge. The language in the existing standard says “consider”, which leaves it to auditor to determine what it means. The Blackstart Plan often doesn’t coincide with CIP standard language.
5. The number of TFEs is currently in the thousands. Processing them is a bureaucratic challenge for regions.

Draft CIP Definitions and Review of CIP Standards

In advance of the meeting, the regional auditors had been provided with a “clean” copy of the latest Reliability Standards on Cyber Security (CIP-002 through CIP-011). They were also provided with the latest set of definition of terms that were being used by the drafting team in preparing the standards.

Each of the drafting subteam leads led the meeting discussions with the auditors on their respective CIP standards. Following a review of the relative CIP Standard by the drafting subteam lead, the auditors were asked to provide their feedback on the requirements, and in particular, their opinion on the auditability of each of the requirements.

A summary of the topics raised and the highlights of the discussions are included in **Appendix 9**. The drafting subteams will consider these comments as they meet over the next month and the full SDT will discuss them during the July 2011 meeting. The SDT will incorporate these comments as appropriate into the Version 5 CIP Standards.

Adjournment

The chair thanked everyone for attending the meeting, either in person or via the conference call facilities, and expressed his special thanks to David Dockery and the AECI staff for doing an excellent job in hosting this meeting at AECI.

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

The meeting adjourned at 4:30 PM on Thursday, June 23, 2011

Appendix #1
Project 2008-06 Cyber Security Order 706 SDT
35th Meeting Agenda
June 21, 2011 Tuesday - 8:00 AM to 5:30 PM CDT
June 22, 2011 Wednesday - 8:00 AM to 5:30 PM CDT
June 23, 2011 Thursday - 8:00 AM to 5:30 PM CDT
AECI Headquarters Building
2814 S Golden Avenue
Springfield, MO 65807

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

Proposed Meeting Objectives/Outcomes:

- Review and discuss major audit issues with current CIP-002 through CIP-009 requirements
- To determine the measurability of draft CIP-002-5 through CIP-011-5 requirements
- To agree on next steps and assignments

Timed Agenda

Tuesday June 21, 2011 8:00 a.m. - 5:30 p.m. CDT

8:00 a.m. **Introduction, Welcome Opening and Host remarks**- *John Lim, Chair & Phil Huff, Vice Chair, David Dockery, AECI*
Roll Call; NERC Antitrust Compliance Guidelines- *Joe Bucciero, NERC*
8:15 **Review of Meeting Objectives, Agenda and Procedures** - *John Lim*
8:45 **Industry Updates** - *Scott Mix, NERC, Mike Keane, FERC and others*
- Cyber Attack TF Report
- DOE/NIST/NERC Risk Management Process
- CIP-005-4 Update
- Other Cyber Security business

9:30 **Overview of CIP Version 5 development and progress –** *John Lim*
10:00 *Break*
10:15 **Overview of Issues Found through CIP Audits –** *Roger Lampila/Tom Hofstetter*
11:00 **BES Cyber System Definitions –** *John Lim*
12:00 *Lunch*
1:00 **BES Cyber System Definitions (cont.) –** *John Lim*
2:00 **CIP-002-5 BES Cyber System Identification Requirements –** *John Lim*
3:00 *Break*
3:15 **CIP-002-5 BES Cyber System Identification Attachment 1 Criteria** - *John Lim*
4:30 **CIP-003-5 Governance Requirements (2) –** *Dave Revill, Georgia Transmission*
5:30 *Recess*

Appendix #1
Project 2008-06 Cyber Security Order 706 SDT
35th Meeting Agenda
June 21, 2011 Tuesday - 8:00 AM to 5:30 PM CDT
June 22, 2011 Wednesday - 8:00 AM to 5:30 PM CDT
June 23, 2011 Thursday - 8:00 AM to 5:30 PM CDT
AECI Headquarters Building
2814 S Golden Avenue
Springfield, MO 65807

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

Proposed Meeting Objectives/Outcomes:

- Review and discuss major audit issues with current CIP-002 through CIP-009 requirements
- To determine the measurability of draft CIP-002-5 through CIP-011-5 requirements
- To agree on next steps and assignments

Wednesday June 22, 2011 8:00 a.m. - 5:30 p.m. CDT

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

8:15 **CIP-004-5 Personnel Security Requirements (4) –** *Doug Johnson, ComEd*
- *R1 - Awareness*
- *R2 – Training*
- *R3 – Training Schedule*
- *R4 – Personnel Risk Assessment*

10:20 *Break*

10:35 **CIP-004-5 Personnel Security Requirements (2) –** *Phil Huff, AECC*
- *R5 – Access Authorization Program*
- *R6 – Access Revocation*

11:45 *Lunch*

12:45 **CIP-005-5 Electronic Security Perimeter Requirements (1) –** *Jay Cribb, Southern Co*

1:25 **CIP-006-5 Physical Security Program Requirements (3) –** *Doug Johnson, ComEd*
- *R1 – Physical Security Boundary*
- *R2 – Visitor Control Program*
- *R3 – Maintenance & Testing of Physical Access Control Systems*

3:05 *Break*

3:25 **CIP-007-5 Systems Security Requirements (5) –** *Jay Cribb, Southern Co*
- *R1 – Ports & Services*
- *R2 – Security Patch Management*
- *R3 – Malicious Code Prevention*
- *R4 – Security Event Monitoring*

5:30 *Recess*

Appendix #1
Project 2008-06 Cyber Security Order 706 SDT
35th Meeting Agenda
June 21, 2011 Tuesday - 8:00 AM to 5:30 PM CDT
June 22, 2011 Wednesday - 8:00 AM to 5:30 PM CDT
June 23, 2011 Thursday - 8:00 AM to 5:30 PM CDT
AECI Headquarters Building
2814 S Golden Avenue
Springfield, MO 65807

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

Proposed Meeting Objectives/Outcomes:

- Review and discuss major audit issues with current CIP-002 through CIP-009 requirements
- To determine the measurability of draft CIP-002-5 through CIP-011-5 requirements
- To agree on next steps and assignments

Thursday June 23, 2011 8:00 a.m. - 5:30 p.m. CDT

8:00 a.m.	**Recap of Day 2, Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Joe Bucciero*
8:15	**CIP-007-5 Systems Security Requirements (5) –** *Phil Huff, AECC* • *R5 – System Access Controls*
8:55	**CIP-008-5 Incident Response Requirements (3) –** *Scott Rosenberger, Energy Future Holdings* • *R3 – Incident Response Plan Review, Update, Communicate*
9:35	**CIP-009-5 Recovery Plans (3) –** *Scott Rosenberger, Energy Future Holdings* • *R1 – Recovery Plan Specifications*
10:15	*Break*
10:35	**CIP-009-5 Recovery Plans (2) –** *Scott Rosenberger, Energy Future Holdings* • *R2 – Recovery Plan Testing Specifications* • *R3 – Recovery Plan Review, Update, Communicate*
11:45	*Lunch*
12:45	**CIP-010-5 Change Management Requirements (3) –** *Dave Revill, Georgia Transmission* • *R1 – Configuration Change Management* • *R2 – Configuration Monitoring* • *R3 – Vulnerability Assessments*
2:20	**CIP-011-5 Information Protection Requirements (2) –** *Dave Revill, Georgia Transmission* • *R1 – Information Protection* • *R2 – Media Reuse and Disposal*
3:15	*Break*
3:30	**Remote Access Urgent Action CIP-005-4 Revisions –** *Christine Hasha, ERCOT*
3:45	**Open Discussion of Version 5 CIP-002 through CIP-011 Standards** • *Review Outstanding Issues & Items* • *Wrap-Up*

Appendix #1
Project 2008-06 Cyber Security Order 706 SDT
35th Meeting Agenda
June 21, 2011 Tuesday - 8:00 AM to 5:30 PM CDT
June 22, 2011 Wednesday - 8:00 AM to 5:30 PM CDT
June 23, 2011 Thursday - 8:00 AM to 5:30 PM CDT
AECI Headquarters Building
2814 S Golden Avenue
Springfield, MO 65807

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

Proposed Meeting Objectives/Outcomes:

- Review and discuss major audit issues with current CIP-002 through CIP-009 requirements
- To determine the measurability of draft CIP-002-5 through CIP-011-5 requirements
- To agree on next steps and assignments

4:45	**SDT Review of July Meeting Agenda and Next Steps**
5:00	**SDT Establish Subteam Meeting Schedule**
5:30	*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
June 21-23, 2011 (Springfield, MO)

Name	Company	JUN 21	JUN 22	JUN 23
1. Rob Antonishen	Ontario Power Generation	X	X	X
2. Jay Cribb	Southern Company	X	X	X
3. Jerry 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. 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. Tom Stevenson	Constellation	X	X	X
12. John Varnell	Tenaska	X	X	X
13. Bill Winters	APS	X	X	X
Valerie Agnew	*NERC Staff*		*X*	*X*
Joe Bucciero	*NERC Facilitator*	*X*	*X*	*X*
Howard Gugel	*NERC Staff*	*X*	*X*	*X*
Tom Hofstetter	*NERC Staff*	*X*	*X*	*X*
Roger Lampila	*NERC Staff*	*X*	*X*	*X*
Scott Mix	*NERC Staff*	*X*	*X*	*X*
Steve Noess	*NERC Staff*	*X*	*X*	*X*

Others Attending In Person or via ReadyTalk and Phone

Tom Alrich, Sharla Artz, Jan Bargen, Bill Beaver, Bruce Bingham, , Stacy Bresler, Dave Burtrum, John Bussman, Larry Camm, Brent Castagnetto, Kathy Daggett, David Dockery, Jay Doran, Tony Durgar, Ryan Ebert, Summer Esquerre, Jerome Farquharson, Stephen Flanagan, Jim Fletcher, Lew Folkersh, Roger Fradenburgh, Doug Freimarck, John Fridye, David Gordon, Kuldeep Hak, Leanne Harrison, Darren Highfill, John Kassel, Dan Kathir, Michael Keane, Drew Kittey, Kim Koster, Patricio Leon, Andres Lopez, Wayne Mackensie, Martin Narendorf, Brian Newell, Dave Norton, Grant Pederson, Kevin Perry, Maggy Powell, Aileen Meyer, Mike Prescher, Bodhi Rader, Ingrid Rayo, Carrie Reimers, Amelia Sawyer, Peter Scalici, Katie Schnider, Sejal Shah, Matt Stryker, Michael Tibbs, Eric Warakomski, Melissa Wehde, Lori Willer

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

CSO706 SDT
Meeting Schedule and Objectives (June 2011)

Meeting Location	Dates	Meeting Objective
Salt Lake City, UT WECC	**7/19 to 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 to 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 to 8/18/2011**	**Review of Standards with Industry Representatives**
Interim Week 1	8/19 to 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 to 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 to 9/9/2011	Update rationale, change documentation and guidance to reflect requirements
Interim Week 4	9/12 to 9/16/2011	Review VRFs and VSLs modified from Version 4 Review CIP-010 and 011 informal comment/response document

APPENDIX #4

CSO706 SDT
Meeting Schedule and Objectives (June 2011)

Meeting Location	Dates	Meeting Objective
Westminster, CA SCE	**9/20 to 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 to 10/14/2011	NERC Quality Review & meeting with DT leadership and subteam leads to provide comments
Interim	10/17 to 10/24/2011	Subteams to review and update standards and all documentation based on QR and prepare for posting
Constellation Baltimore, MD	**10/25 to 10/27/2011**	**SDT Meeting to consider QR changes made to the standards and finalize standards for posting**
Interim	10/28 to 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 to 12/19/2011	Version 5 CIP Standards 45+ day formal Comment and Ballot Period
	11/4 to 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 to 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***

APPENDIX #4

CSO706 SDT
Meeting Schedule and Objectives (June 2011)

Meeting Location	Dates	Meeting Objective
		through CIP-011 Standards
Web Conference	**11/30 to 12/1/2011**	**Drafting Team Meeting to review Webinar questions and comments**
	12/20 to 12/21/ 2011	NERC Staff Prepares Industry Comments and Ballot Comments Received for Review by SDT
Review Comments	12/22/2011 to 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 to 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 to 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 to 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 to 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 to 3/9/2012	NERC Quality Review of Responses to Industry Comments from 45-day comment & ballot period. Quality Review of related updates to the CIP standards

APPENDIX #4

CSO706 SDT
Meeting Schedule and Objectives (June 2011)

Meeting Location	Dates	Meeting Objective
Interim	3/12 to 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 to 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 to 3/23/2012	NERC Prepares Documents for Successive Ballot
POST Responses to Comments	*3/26/2012*	*Post responses to 45-day formal comments with concurrent ballot comments*
Comment & Ballot	*3/26 to 4/27/2012*	*30-day Posting of CIP Standards for comments with successive ballot*
Interim	3/26 to 4/25/2012	Begin preparation of FERC filing documentation
Interim	4/30 to 5/1/2012	NERC Staff Prepares Industry Comments and Ballot Comments Received for Review by SDT
Interim	5/2 to 5/22/2012	Subteam meetings to prepare responses to successive ballot comments and revise text of CIP Standards, as necessary
Location (??)	**5/22 to 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 to 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	6/11/2012 6/22/2012	Recirculation Ballot
Finalize Standards	*6/25 to 6/29/2012*	*Finalize CIP standards text for approval by NERC BOT*

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.

CIP Standards Development Overview

June 21, 2011

John Lim

Appendix #9

Auditor Comments Summary

Project 2008-06 CSO706 Cyber Security Standards
Auditor Input and Comment Summary
CIP-002 through CIP-011 (Version 5)
Drafting Team Meeting – Springfield, MO
June 21-23, 2011

Issues found with current audits

· Tom - Issues in audit have more to do with the way organizations are set up. CIP compliance is distributed throughout the organization.

· Tom - CIP-006 R1.1, six-wall boundary requirement

· Tom - "Consideration" of Blackstart Resources - There are issues with the word "consider". What does that mean?

· Tom - Number of TFEs in the 1000s. It has turned into a bureaucratic challenge.

· Kevin - Some requirements are not auditable - password complexity is overly prescriptive. How do I audit the complexity an individual has in their password (i.e. procedural enforcement of passwords)

· Definition of annual in the Standards - addressed in the CAN, but this is not very helpful

· Matt - Ports and services at the boundary and endpoints have been problematic

· Kevin - Provisions of the CAN needs to be included in the Standards

· Bill - Segregation of duties is lacking in the Standards (i.e. if you make a change, you cannot promote the change)

· Matt - "consider", "as necessary", "readily available" are difficult terms to audit.

· Tony - What does "implement" mean? If implement is a performance audit, it needs to be specified.

· Kevin - Get away from explicit specification and move to goal-oriented requirements. One example is to focus on the goal of password requirements rather than parameters for specificity.

· Lew - "Essential to the operation" for CCAs can be interpreted as single point of failure, and this was not the intent. Be careful with the terminology

Appendix #9

Auditor Comments Summary

Broad Issues with Version 5

· Lew - use "individuals or persons" instead of Personnel

· Bill - Preamble - change to "include all the required items" and "for each of their BES Cyber Systems"

· Lew - Applicability column is confusing when switching to personnel

· Kevin - For applicability column with authorized personnel, tie it to High/Med Impact Systems and specify any scoping filters within the requirement statement (i.e. persons with access to…)

· Kevin/Lew - Modify all retention requirements to ensure evidence available since last audit period.

· Winters - Limit the degree to which auditors need to apply quality and effectiveness judgments.

· Tony - How are we going to execute the plan to audit these requirements (CMEP - risk-based monitoring)

Appendix #9

Auditor Comments Summary

Definitions - Cyber Asset, BES Cyber Asset, BES Cyber System

· Matt - Attachment 1 criteria is very specific. The same is not true for CCA/BES Cyber Asset. How does an auditor determine what is a BES Cyber Asset. It seems very difficult to identify BES Cyber Assets on a large scale. The theory sounds very good, but it seems difficult in practice.

o Rosenberger - Some of the functions are easier to identify

· Kevin - Do not see where the issue of redundancy is addressed. Can an entity say an asset is not critical because they have a redundant system?

· Kevin - Instead of tying to a specific time interval (15 minutes), tie it to the function. Concern with focus on real-time without considering the loss of integrity. Entities may take advantage of the 15 minute rule

· Peter - What is the rationale for changing the terminology such as BES Cyber System and Physical Security Perimeter

· Lew - The auditor will be looking for at the assets an entity has not identified. The concern is not so much with the cyber assets an entity has identified as BES Cyber Assets. Does not have any ideas on improving this approach.

o This is a very extensive approach to auditing. There needs to be some level of trust in the audit.

o Regions must operate under the requirement of "trust but verify"

· Matt - How do you consider "misuse" in the assessment of Cyber Asset? Need more parameters/guidance to make it clear.

· Perry - He thinks the list of real-time reliability functions does a good job at limiting the scope of Cyber Assets

· Perry - The concept of data in motion is missing in these definitions.

o Not trying to address data-in-motion in this definition

Open Discussion

· Darren Highfill - The definition of BES Cyber Asset is redundant in "executing one or more reliability operating functions". The first qualifier seems redundant to the bullet points in the definition.

Appendix #9

Auditor Comments Summary

Definitions: Control Center

Open Discussion

· John Bussman - Are relay tech laptops considered a Control Center?

o Opening paragraph includes "real-time operations by System Operators" - This is meant to limit to the traditional definition of Maintenance.

o Kevin - need to fix the problem of new maintenance devices. Need to have controls around maintenance devices.

· Scott Mix - Need to address Control Center for generation control rooms and transmission substations where devices may control one or two other assets.

Definitions - ESP, Physical Boundary, BES Cyber System Information, and other subject-matter specific definitions

· Kevin - (Physical Boundary) Rationale on the change from PSP to Physical Boundary. It seems difficult to apply this definition and potentially many different interpretations.

  o The intent was to focus on how you are protecting the boundary and not that you must have a wall.

  o It's best to look at this definition in conjunction with the requirements of the Standard

· Bill - (Physical Boundary) Likes this definition because it allows entities to have mitigating controls.

· Matthew - (Physical Boundary) It might be helpful to define physical border as 3-dimensional

· Kevin - (Physical Boundary) You could do away with this definition if you made your Standard requirement more goal-oriented. State the goal is to prevent access and let the entities surprise you with ingenuity and the auditor surprise you with subject matter knowledge.

· Pete - (Physical Boundary) There have been places I've seen where a navy seal could not get in, but they are out of compliance because the requirement is unreasonable. Agreement in just doing away with the definition.

· Kevin - (Maintenance)2 types of devices we have seen in audits for maintenance. "Intended purpose device" that stays on all the time to allow them to perform maintenance should be considered CCAs, but roaming laptop would be considered a temporary device.

· Kevin (Maintenance) - Make sure you have addressed the risk mitigation for maintenance devices.

  o Revill - That is our intent with the maintenance devices.

· Martin Narendorf (Reportable Cyber Security Event) - This definition seems overly broad.

  o Scott Rosenberger - The event without anything else happening would be within this definition

Appendix #9

Auditor Comments Summary

- o Kevin - Mixed tense within the definition could be the cause of confusion. Modify to say "had the potential…"

- o Christine Hasha -Need to be aware of EOP-004-2 developments.

· Lew (Reportable Cyber Security Event) - Why the change from Incident to Event

- o The focus is on reportable events

· Matt (Protected Cyber Assets) - The term "directly connected" is not interpreted as "on the same network as"

· Kevin (Protected Cyber Assets) - Reword to same side of your "Electronic Access Point" as other BES Cyber Assets.

Appendix #9

Auditor Comments Summary

Definitions - Reliability Functions

Open Discussion

· Kevin (Situational Awareness) - Very dependent on the entity. Any information needed for real-time operational decisions.

· Darren Highfill (Sit. Awareness) - This may significantly expand in scope in the future when devices like PMUs come online.

· Leann Harrison (Sit. Awareness) - Break down what this means per registered entity. What does Sit. Awareness mean for GOP as compared with TOP?

· Kevin (Sit. Awareness) - TOP-005, TOP-006, IRO-003, IRO-005 and potentially others to define Situational Awareness.

Appendix #9

Auditor Comments Summary

CIP-002

R1:

- Clarify responsibility for categorization (owner/operator)
- Planned:
  - Use permanent instead?
  - Include time frame: intended to be in place for more than 6 months, e.g.?
- Completion of change: commissioning/energized/in operation?
- What is a change
  - To what: BES Facilities, element
  - How to qualify in scope changes for triggering review

M1:

- Include list of changes to the BES

R2:

- Specify annual
  - At least once every calendar year not to exceed 15 months between occurrences
  - At least once every 12 months
  - Consideration for general definition?
- Include consideration of **null lists**
- Simplify structure and language

Attachment 1

- BES Cyber Systems "that can affect operations for" : consider using language in definition
- 1.1: Control Center - capitalize defined term
- 1.2: should this be consistent with 2.1 (aggregate MW) (probably not, check BAL functions, standards)
- 1.4: same as above : probably yes
- 2.5: up to **and including** the point…
- 2.8: Obligation of RC, PA or TP to notify owners of IROL qualified Facilities? Verify (probably in guidance document for version 4, to be checked)
- 2.10: evidence of communication from GO/GOP to TO ?
- 2.14: Control Centers outside of NERC jurisdiction that control qualified BES Facilities in NERC footprint.
- 3: Low: remove "documented" ; no requirement to document Lows.

Appendix #9

Auditor Comments Summary

CIP-003

R1:

- It would be useful to add specific objective criteria to the policy to improve the auditability.
- The governance for Emergency situations has been removed. Consider reinserting this in the policy area.

R2:

- Add measure that indicates that workflow evidence (such as SharePoint) would be acceptable.
- "Signed and dated" is considered the gold standard for evidence. Use this throughout.
- Consider correcting the bookending issue by also requiring "initial" approval.

R3:

- Personnel tends to imply only the employees of a company. Consider using persons or individuals instead.
- What is really meant by accessible in this scenario?
- Individuals with "access to" is easy to define, however "responsible for" is not. Consider removing "responsible for."

R4:

- Consider making this requirement R1 since the senior manager is used before.
- Consider if this needs to be a more formal declaration or clarify that the senior manager cannot just assume this role.

R5:

- Consider if the delegation needs to specify specific functions or if a general delegation is acceptable. Make this clear in the measures.

Appendix #9

Auditor Comments Summary

CIP-004

- Consider use of “individuals” in place of “personnel”
- Address use of Annual (At least once per calendar year, but not to exceed 15 months between [*occurrences*])
- Change rational out of sync with several table items
- For Applicability spell out Responsible Entity instead of using RE abbreviation

R1:

- Communicate to whom

R2:

- Entities have had a hard time on “proper use”
- Expand guidance to provide examples
- For guidance and measure should include requiring a list of roles with which modules each role must get
- Clarify better what our expectations are
- Can an entity have just one training module for everyone?
- Liked the addition of visitor control to training

R3:

- Table names and titles out of sync
- “impact on reliability” in emergency response clause,
- require documentation on when emergency response clause has been invoked
- general comment, relook at applicability, personnel are not registered so should be RE and then have personnel referenced in the Requirement wording
- Include “all of the required”, or “all items” in the requirement wording
- Concern about lack of overarching emergency provision process in CIP-003
- 3.3 what is training opportunities and how is it audited? don’t do this as a requirement

R4:

- The applicability should be the same for whole table
- Trouble requiring Photo ID – consider using I9 for which documents to accept
- Does (Federal, State or Provincial) apply to both Or clauses?
- 4.2 use shall or must instead of “should”
- 4.3 change rationale is better than the requirement, consider using that instead
- 4.3 change to “criteria or process used”
- 4.4 documenting this is going to be problematic
- 4.4 personal should be personnel
- 4.5 issue with “its personnel”, should have documented results for everyone, it might be just an attestation from the vendor

R5:

- Table names and titles out of sync
- Provide examples
- Reference CIP version 1 FAQ document for good example
- Use wording such as “Update each PRA …. No later than 7 years after the last PRA”

Appendix #9

Auditor Comments Summary

- 5.1 Suggested measure would be "Example may include redacted PRA records showing person's name and date of completion (see guidance document)"
- 5.2 Suggested measure would be "Current and former PRA records"
  - Kevin: - Need to make sure actual rights are appropriate and actually needed
    - 6.1 – Why "external connectivity" limitation?
    - Make sure access control & monitoring systems are addressed
    - 6.4 and 6.5 – what's difference between what's required?
      - Needs to be clearer
        - Who has an account (or access) vs. who's got what privileges (where different privileges exist)
    - 6.5 - immediate revocation might not be the right course in all cases – it might be "fix your records"
      - Use "Group or role" consistently throughout
    - 6.6 – As written, suggests you MUST update documentation
      - Might not be necessary (measure is better)
  - Matt:
    - 6.4 – how to measure "same day"?
      - Suggests 24 hour as more measurable
        - Phil noted we've tried to get away from hour-based reqmt
        - Could we say, "same or next business day"?
    - 6.4 and 6.5 – Measures *appear* to be written in a way to avoid violations
      - Language of requirements needs to be clearer if that was our intent (it was)
  - Bill Beaver: - suggests use of "system generated reports" as the authoritative source of who's got what access & privileges
    - Where supported by the BES Cyber Systems
    - Including 6.4 (Christine Hasha from ERCOT thought it was only a verification of authorization)
  - Pete (NPCC): - thinks 6.4 and 7.2 collide
    - But he thought 7.2 was "the" revocation process allowing 7 days
    - **We need to consider revocation on the 1st and a quarterly review on the 3rd**
      - Need to make sure they don't step on each other (they shouldn't, but…)
    - 6.4 needs to be clearer per Kevin
  - Lew: - "Simple & Elegant" language is nice but "brute force" may be needed in some cases to audit
    - e.g., 6.1 – not sure he could audit – thinks it's too "gray"

- Phil resists "least privilege" – Kevin suggests adding language to the effect that only privileges needed to perform assigned work functions

- Doug J: -We're trying to get away from "zero defects" and towards goal-oriented requirements.
  - Can auditors help?
    - Kevin's concerned about the risk associated with somebody still having access after it should've been revoked.
      - But isn't there a difference between, say, a termination and a transfer in terms of degree (of risk)?

- Discussion seemed to then go towards trying to draw a distinction between "failure to revoke" and "access by mistake" with only the former being a violation.

- Matt S: - suggests that we might consider writing requirements around some sort of thresholds for frequency of reviews, number of mistakes found, over what period of time, before the first (N) mistake(s) are considered violations?

R7 Revocation

- Matt S: - Measures should include system log file records
  - Doesn't think "workflow" info is very strong evidence
  - Also thinks time/date info should be included

- Lew: -7.1 is unenforceable without "when" info
  - Current "when" is a trigger – how much time for response?
    - Matt and Kevin agree something, perhaps "same or next day" or "within 8 hours"
  - Also concerned with vagueness of "actions necessary"
    - e.g. just pulling a badge was cited as an example of an insufficient process
    - Suggests some of the language in measures might be better incorporated into the requirement statement(s), like it or not
    - Kevin: - Suggests, "take necessary steps to *deny* physical and electronic access"
  - Several people, including Kevin, Lew, Mike K, like the idea of *going back to* our earlier use of "primary and secondary access"
    - So 7.1 could say, "remove primary access"

- Kevin: - What happened to transmission facilities in 7.2?
  - We dropped them due to the problem of entities with hundreds of substations and thousands of relays
    - Kevin: - Understand the problem but we can't simply not address it
  - Need to make sure ALL types of accounts are addressed, include O/S, database etc.

- Kevin 7.1:
  - Addresses BES Cyber System Information – Do we intend to require entities to use some sort of information rights management system?
    - How would "further access" be prevented?

- We should pull info access out and put into its own reqmt

- Kevin: - Data retention
    - Use same language that's in CIP-002 is in ALL stds!!!
    - Discussion of "90 days"
        - Scott M: - Need to keep log files IF they're what you're using to demonstrate compliance

- Lew: - Once more, keep in mind auditors can only audit to requirements, NOT to measures or guidance
    - Clearly thinks some of the language in 7.1's current "measures" should be in the actual requirement
        - So does Matt S.

Phil's Notes

- Kevin - Need to make sure entities review the access rights in the privilege review.
- Kevin - Access control and monitoring devices not in the applicability section
- Kevin - Not clear the differences between the authorization and privilege reviews
- Kevin - 6.5, they may need the access, an additional appropriate action would be authorize access where appropriate
- Kevin - 6.6, it may not be necessary in some instances to update the document.
- Matt - Use 24 hours instead of "same day" or consider business day to move away from hours.
- Matt - Make the intentions very concrete that issues discovered during the review are not findings.
- Bill - Use system-generated reports as examples of evidence in 6.4 and 6.5
- Bill - Evidence for authorization would be system-generated reports, 6.1 and 6.2
- Lew - "Grant only access and privileges necessary to perform assigned work function"
- Pete - Need to revisit the issue where having 7 days to revoke access does not overlap the quarterly review
- Matt - Consider prescribing something more strict in the review as part of the process improvement in 6.6. Need a clear path of mitigation rather than going through the enforcement process.

Revocation of access

- Matt - Add to the measure something about evidence the person was actually removed from the system.
    - This might be addressed in bullet 3.
- Lew - There is no timeframe tied to 7.1 on revocation. Difficult/impossible to audit
- Lew - Need more specification about preventing further access. Difficult to audit.
- Perry - Suggested wording, "upon termination within x timeframe, take steps to deny physical and remote electronic access to BES Cyber System"
- Perry - Prevent access to BES Cyber System Information is infeasible
    - Separate the BES Cyber System Information requirement and be more specific about what revocation means.

Appendix #9

Auditor Comments Summary

CIP-005

R1:

- Work on circular definition – Electronic Connectivity and ESP – needing an ESP to determine whether you have Electronic Connectivity in order to define the ESP.
- Redo the measures on 1.2 – ping sweeps very weak.
- Consider defining routable protocols – get it out of the FAQ and include IPV4 and IPV6, TCP and UDP, etc.
- Consider wording on 'default deny rule' and how that works with Cisco devices with their implicit rules.
- Work 'business or operational justification' into EAP rules.
- Consider expanding requirements around dial-ups to include all temporary connectivity.
- In 1.5, consider how to handle encrypted traffic travelling through the EAP.

Appendix #9

Auditor Comments Summary

CIP-006

- Wording in change rational out of sync with several table items
- Define what Annual means
- Measures should not be written with “verify that”
- Felt this version is considerably weakened from previous versions due to lack of “how” in requirements

R1:

- Consider using “restrict” instead of “control”.
- Provide examples of control
- Add requirement to identify the access points
- Address zero defect issues - 7 days a week 24 hrs a day – possibly use wording similar to BAL-005 R8.1 to establish a availability factor
- 1.1 can’t do both, change wording to be “operational and/or procedural”
- 1.2 how is this different than 1.3 and why are Electronic Access Control Systems protected different than the other PSPs
- 1.2 should not allow technical feasibility exception
- 1.3 Provide guidance and multiple examples of “different and complementary physical access controls”
- 1.3 Does using the same control system for two different controls qualify
- 1.4 is this to monitor for attempted or actual access attempts
- 1.4 provide a time frame for the immediate notification, this has not been a problem in recent audits
- 1.4 24 hr seven days a week allows for no equipment failures without violations, address to eliminate zero defect
- 1.4 measure, suggest “demonstrate that alerting has occurred”
- 1.5 when do the reviews need to be done, provide a time frame
- 1.6 does “log … access through any defined boundary” mean entry or both entry and egress.
- 1.7 Clarify what is required, is it authenticate person or authorization of people who can have access.
- 1.7 Is there a risk that unauthorized unescorted physical access could cause a violation? Make the language crystal clear.

R2:

- What does “continuous escorted access” mean, this has been an issue in audits, does it mean line of sight, close enough to tell what they are doing, etc.
- Define what desired outcome should be
- Consider “active escort” which could mean “be aware of what the individual is doing in the proximity of the protected cyber assets”
- Visitors identity, how do you confirm and differentiate between people with same name
- Does the escort have to have documented training per CIP-004?
- How do they audit that the escort has occurred if the escort is not identified in the log
- Potential problem with first in and last out logging, what if they think they will be returning but never return to close log entry
- What is the NRC requirements for escort logging, (see 10CFR073-55)

Appendix #9

Auditor Comments Summary

R3:

- Believe even annual testing is not enough
- Separate testing and maintenance so different time frames can be specified
- Suggest wording such as “Prior to commissioning and following a cycle no longer than…”
- 3.1 mechanism is not a term used in other parts of CIP
- 3.1 Consider if previous wording needs to be brought back in.
- 3.2 & 3.3 consider handling in the data retention records section and align with audit period
- Suggest wording that testing is “to ensure all devices are functioning correctly”

Appendix #9

Auditor Comments Summary

CIP-007

R1:

- Consider naming network, serial, and USB ports as the physical ports we care about (to eliminate keyboard, mouse, etc).
- In 1.1, need much more clarity around where the disabling of logical network ports is to be implemented – at the device and at the EAP. Looks to be at the device only. Consider the 'Disable listening ports' language.
- Consider the interplay between services and ports. Can we combine them into one, disabling those services that have listening ports that are not needed. Must address services that can not be disabled and OS'es that are not Windows/*nix based.
- For 1.3, consider rewriting in an outcome based way. What is the desired outcome of restricting access to physical ports.

R2:

- Tie the source of software patches to the config mgt in CIP-010.
- Consider the source of patches and the vulnerability time between when Microsoft announces the patch and the vendor OK's the patch.
- Separate back out the assessment of the vulnerability and the mitigation (with a timeframe) and the implementation of the patch. Put some kind of timeframe on the eventual implementation of the patch.
- Move the 'dated implementation plan' from the measure to the requirement.

R3:

- Consider the 'Deter the introduction and propagation of" language. Make it more outcome based.
- In 3.4, consider timeframes for signature updates – how stale is too stale? Also address testing of updates with the goal of not harming the availability of the system.

R4:

- Make sure 4.1 doesn't read as a zero defect (must never have logging downtime).
- Add clarity around 'audit processing failures'
- Add clarity around the 'must log' events – successful and failed user logon/logoff, etc. Remove 'user activity' – too vague.
- In 4.2, insure that the actual generation of alerts is required.
- Add elements for a 'quality' review of log samples (signed and dated, etc)
- Insure we don't have recursion on the real time alerting on the real time alerting system failures.
- Make sure the timeframes for retention are not just "90 days" but "at least 90 consecutive calendar days"
- In 4.5, how do screen shots show that the logs are actually being retained?

R5: Passwords etc.

- Matt S:
    - "Special" characters not well-defined – suggests something a bit more specific & bounded
    - 5.3 Currently no TFE available in the Stds – acks it's hard
    - 5.2 Suggests adding account types to requirement
        - Howard explained why we prefer it in guidance

- 5.4 – Maybe too open, flexible. Perhaps establish some sort of minimun password entropy requirement
    - (How would that be audited???)
        - Ans = It's do-able with relatively simple tools
    - **John Lim believes the subteam considered it once, way back…
        - Ask Sharon?
    - Howard notes that many field assets don't enforce entropy
    - If we want to allow for procedural enforcement, say so
- General concern = Time required to audit may grow as entities are given more flexibility in how they address a given requirement

- Lew:
    - Can't audit reqmt in any meaningful way
        - 5.4 allows entity to make the call on length, complexity, etc.
        - 99% of entities will do the right thing, but we can't audit it
            - Phil – How would 800-53 be audited?
            - Lew – FISMA audits are very different than CIP
- Lew: – What is SDT aiming for here?
- Me: - If passwords used, use strongest ones possible
- Dave Norton: - Should have a lockout provision to protect against high-powered cracking
    - Should also apply to Low
- Kevin:
    - Be careful about using "entropy"
        - Will not be well-understood everywhere so be sure to define it
    - Where lockout is available, use it
    - Don't allow same-day changes
    - Length: Pick one you like
    - Say "Minimum of ___" or longest available
        - Do the same with complexity
    - If you use certs, make sure they expire at some point
    - 5.1:
        - Think about requiring multi-factor auth for high
        - Say "authenticate user before granting access"
    - 5.2
        - Measure 3 How would "acceptable use" be enforced? Think about removing this
    - 5.3

  - Keep in mind "Microsoft" is a vendor – IWAM (??) – be sure we're clear about what we mean (e.g., make sure default passwords in an app are changed)

- Darren Highfill:
  - Concerned that saying, "if passwords used, use X strong or strong as possible," can leave the door open to entities providing only pretty weak protection – Not serving goal of better security – How about mitigating measures?
- Kevin: - Good goal but can lead to needing subjectivity in audits

CIP-007 R5 (System Access Controls)

1. Suggest adding more definition to "special characters."
2. 5.4 may be too flexible – suggest considering use of a minimum entropy requirement for passwords
   - It was noted that "entropy," if used, would have to be clearly defined
3. If we want to allow for "procedural" enforcement of various rules around various types of authentication, we should make it clear
4. 5.4 not auditable as written – entities would be able to decide for themselves what password length and complexity requirements should be used
5. (Suggestion from Dave Norton @ FERC) If passwords used there should be a lockout requirement after "N" failed tries to protect against cracking tools
   - Should apply to Low BES Cyber Systems, not just Med and High
6. Suggestions for password rules
   - Don't allow same-day changes (so a lazy user can't change his back to the one he's been using)
   - Suggest using phrasing like "minimum of X characters or longest available" and similar phrasing for complexity
7. Other suggestions
   - Consider requiring multi-factor authentication for High systems
   - Consider saying, "authenticate before granting access"
   - If digital certificates are used, they should expire at some point
8. Consider deleting 3rd measure for 5.2
   - How would "acceptable use" be enforced?
9. Suggest being clear that 5.3 is referring to default passwords in applications

Appendix #9

Auditor Comments Summary

CIP-008

- 1.1 Physical events also? Tornado? Need to clarify that there are Cyber events
- 1.1 Consider the following intro: A process to identify cyber events as reportable Cyber Security Incidents. Reportable Cyber Security Incidents are those cyber events are:
- 1.2 Communication plan – what does this mean? Communicate to whom? More clarity
- 2.1 Address responding to incidents without using plan – requirement to implement or follow (FERC 694 for CIP-009)
- 2.1 Testing should consider requiring the use of a BES Cyber Systems or Asset (Measurement? – test using Assets covered by CIP standards?)
- 2.1 Should the External Communication by tested? (overlap with EOP-004?)
- 2.1 Timing 12 months – consider every calendar year not to exceed 15 months
- 3.1 clarify if review included EOP-004 communication review

Appendix #9

Auditor Comments Summary

CIP-009

- 1.1 Specify what a Recover Plan includes (some wording to tie to BC/DR Concepts)
- 1.1 Address recovering without using plan – requirement to implement or follow (FERC 694 for CIP-009)

- 1.2 Consider clarifying that Recover Plan is to restore function or system
- 1.3 What does protection mean? Consider in guidance?
- 1.4 Testing of Backups – Only initially? After each backup? Possibly additional clarity is needed
- 1.6 More clarity on the purpose of Data Preservation. Possibly in Guidance?

- 1.3 2.3 How to insure that all of the information software, data, etc is available to recover all Bes Cyber Systems. Guidance or requirement? Should testing process include consideration of findings on a broad basis across all BES cyber systems?

- 2.1 Testing should consider requiring the use of a BES Cyber Systems or Asset (Measurement? – test using Assets covered by CIP standards?)
- 2.3 should shall be shall or should shall not be should. Make it a must do.
- 2.3 operational exercises – should this be a FULL operation exercise? Should language be included to clarify how big this should be or how small it can be?
- 3.2 60 months to match CIP-008

Appendix #9

Auditor Comments Summary

CIP-010

R1:

- Consider additional items for the baseline configuration such as date of deployment, IP address, hostname, patch level, logging configuration, malicious software prevention tools (if any), authentication method and settings.
- Ensure clarity of what types of changes must go through the change management process.
- Determine if there needs to be a defined window in which the testing must occur.
- Ensure the consistency of language in R1.3: assess vs. verify vs. test.

R2:

- Consider rewording this requirement to include manual reviews of a defined frequency in order to prevent unnecessary TFEs.

R3:

- Additional guidance is needed on what is meant by "review," "passive vulnerability assessment," and "active vulnerability assessment."
- Ensure clarity on whether physical security controls are also covered as part of the vulnerability assessment.
- Add language to ensure that known access points are covered by the vulnerability assessment as well as the discovery of unauthorized access points (wireless or otherwise).
- Consider correcting the bookending issue by also requiring "initial" vulnerability assessments.
- Testing of new cyber assets should be performed on the asset itself prior to deployment and not just in a test environment.

Appendix #9

Auditor Comments Summary

CIP-011

R1:

- Correct the inconsistencies between the measures, change rationale, and the requirements.
- Consider establishing a “floor” as to the minimal acceptable handling and access control requirements.
- Clarify the connection between the access control requirement for BES Cyber System Information and the requirement to authorize access in CIP-004.
- Consider a requirement that covers what to do if information that should have been protected in released to an unauthorized individual.

R2:

- Evaluate the measurement language that indicates an “acceptable method.” This could potentially lead to inconsistency among the regions as to what is considered acceptable.
- Consider the situation of the PC used for vulnerability assessment purposes and how that will be handled with respect to the media sanitization requirements.
- The development of guidance in the area of media sanitization would be very beneficial.
- Add examples of gold star evidence to the measures that include the date of destruction along with a device specific identifier.

Appendix #10
Meeting Evaluation Results
June 21-23, 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		