NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706
33rd Meeting Summary

Sacramento, CA

Tuesday, April 12, 2011 |8 a.m. to 6 p.m. PDT
Wednesday, April 13, 2011|8 a.m. to 6 p.m. PDT
Thursday, April 14, 2011|8 a.m. to 6 p.m. PDT

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
33RD MEETING
April 12-14, 2011
Sacramento, CA

Executive Summary

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to the Sacramento Meeting of the CSO706 SDT, and thanked them for their participation in this meeting. John also acknowledged Kevin Sherlin, the meeting host, and his Sacramento Municipal Utility District (SMUD) Team for all of their efforts in making this meeting possible. Kevin 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 day. On Tuesday morning, the SDT unanimously adopted the March 15-17, 2011, New York, NY 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-009 requirements, review of the implementation plan concepts, and agreement on the team's next steps and assignments. **Appendix 1** contains the meeting agenda.

The Chair reported that team still desires another Canadian representative, which is posted as a vacancy for the team. He also announced that Bill Gross has resigned from the Standard Drafting Team, but will continue to follow its developments. **Appendix 2** contains the meeting attendance list, and the current drafting team roster is part of the meeting agenda packet.

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 based management 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 was out for industry comment and ballot, with the ballot results due on April 28th. If the new standard does not gain an affirmative ballot, it may be a possibility for the CSO706 drafting team to pick up this work since the concepts need to be addressed in V5 of the CIP standards.

Scott also reported on the IEC 61850 standard discussions and guidelines concerning the applicability of 61850 to all devices with routable protocol (IP) addresses. Scott is concerned about their schedule and the current level of coordination with the CIP standards.

Drafting Team Schedule

The drafting team reviewed the current project and meeting schedule (See **Appendix 3**), and the team discussed possible meeting dates, objectives, and locations. The team decided to target the June 2011 meeting to have an open session with representatives from the Regional Audit teams in Springfield, MO at AECI's facilities to review an early draft of the next version of the CIP Cyber Security Standards. The drafting team also targeted the August 2011 meeting to meet with representatives from the industry trade 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 project schedule for the team to review in Little Rock.

Subteam Assignments

The current makeup of each sub-team is provided in **Appendix 4** for reference.

Needs, Goals, & Objectives

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

Format of CIP Version 5 Standards & Framework

The SDT reviewed the Mapping document that was developed and adopted at the March 2011 meeting, and it is provided in **Appendix 6.** This document describes the mapping of the previous version of CIP-010 and CIP-011 to CIP-002 through CIP-009. It was decided that a couple of the previous CIP standards had too many requirements within them, and they should be separated into multiple requirements thereby expanding the CIP standards into new CIP-010 and CIP-011 requirements.

The SDT reviewed the format that will be used in developing the updated version (Version 5) of the CIP standards. John Lim created a draft framework for the Version 5 standards and reviewed this with the drafting team for their comments. The requirements in CIP-002 and the measures for those requirements are now placed next to each other in the revised format. The suggested CIP-002-5 framework document is provided in **Appendix 7** for reference.

The drafting team also discussed the proposed contents of the tables that further describe each of the requirements and the associated sub-requirements. The team resolved that the requirements should be action (verb) oriented, and the measures should be more "noun" oriented. Further, the rationale statements that are currently in text boxes could be pulled out into a separate section of the document.

CIP-002-5 Subteam

The BES Cyber System Categorization sub-team presented its latest version of CIP-002 revisions to the drafting team. John Lim and the CIP-002-5 subteam (consisting of Rich Kinas, Mike Keane, Jim Fletcher, and Dave Revill) will continue to meet in the weeks ahead to refine the requirements for CIP-002-5.

John Lim (the Chair) also presented a mapping of the CIP-011 standard into a proposed CIP-003 to CIP-00x format, with two new standards being needed to foster meaningful reorganization of the CIP standards.

Style Guide

Phil Huff provided a summary of his review of the CIP standards, and his recommendations for an updated style guide for all of the CIP standards to follow. The style guide is included as **Appendix 8**. Some of the highlights are: to keep the requirements simple in nature; be specific as to what is needed for evidence in the measures; only provide one measure per requirement and sub-requirement; and be careful not to introduce a new requirement in the measures.

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 few weeks and finalize their respective draft requirements.

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?

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.?

Review of FERC Data Request of NERC (Docket RM11-11)

Scott Mix announced that FERC had issued a data request of NERC as it reviewed the proposed CIP Version 4 standards (**Appendix 9**). Some of the questions will require input from the industry, while others can be addressed by NERC. FERC has asked for a summary of responses by region, but NERC will need to ask individual entities for their data inputs and then summarize the responses by region for FERC.

A request for an extension of 45 days has been submitted to FERC, since the initial requested submittal date of June 1 was already in jeopardy. The extension would move the submittal date to July 11, 2011. The data request will likely extend the FERC Order date regarding CIP Version 4 standards beyond September 2011.

Howard will likely lead the data survey effort, in light of his work previously performed on the Section 1600 data survey.

Subteam Meeting Schedules & Full SDT Discussions

Each of the subteams scheduled their respective meetings between now and the Little Rock meeting in May 2011 to continue the development of their respective standards, measures, and VSL/VFRs.

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 Trade Representatives.

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

1. Provide the latest draft of the standards by the end of May 2011 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 sesions
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 to be sent to the participants ahead of time.

Implementation Plan

A subteam is needed 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 defines. A single date for all would likely mean a long time frame since there will be plenty of work to perform. 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 Kevin Sherlin and his support team for their excellent job in hosting another meeting at SMUD.

The meeting adjourned at 4:30 PM on Thursday, April 14, 2011

Appendix 1

Project 2008-06 Cyber Security Order 706 SDT
33rd Meeting Agenda
April 12, 2011 Tuesday - 8:00 AM to 6:00 PM PDT
April 13, 2011 Wednesday - 8:00 AM to 6:00 PM PDT
April 14, 2011 Thursday - 8:00 AM to 6:00 PM PDT
Sacramento Municipal Utility District (SMUD)
6201 S Street, Sacramento, CA 95817

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

Proposed Meeting Objectives/Outcomes:

- To review CIP V5 multiple standard format and standard/requirement mapping (CIP-002 – CIP-00X)
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To review and finalize style guide for drafting of CIP requirements
- Initial draft of CIP-002-5 through CIP-009-5 Requirements
- To review and discuss implementation plan concepts
- To agree on next steps and assignments

Timed Agenda

Tuesday April 12, 2011 8:00 a.m. - 6:00 p.m. PDT

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

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

8:20 **Industry Review**- *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

8:50 **Review of CIP V5 Multiple Standard Format and Mapping** – *John Lim*

10:00 *Break*

10:15 **Review of CIP-002-5 impact levels –** *John Lim*

12:00 *Lunch*

1:00 **Review of CIP-002-5 Standard -** *John Lim*

3:00 *Break*

3:15 **Review of Style Guide –** *Phil Huff*

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

6:00 *Recess*

Appendix 1

Project 2008-06 Cyber Security Order 706 SDT
33rd Meeting Agenda
April 12, 2011 Tuesday - 8:00 AM to 6:00 PM PDT
April 13, 2011 Wednesday - 8:00 AM to 6:00 PM PDT
April 14, 2011 Thursday - 8:00 AM to 6:00 PM PDT
Sacramento Municipal Utility District (SMUD)
6201 S Street, Sacramento, CA 95817

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

Proposed Meeting Objectives/Outcomes:

- To review CIP V5 multiple standard format and standard/requirement mapping (CIP-002 – CIP-00X)
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To review and finalize style guide for drafting of CIP requirements
- Initial draft of CIP-002-5 through CIP-009-5 Requirements
- To review and discuss implementation plan concepts
- To agree on next steps and assignments

Wednesday April 13, 2011 8:00 a.m. - 6:00 p.m. PDT

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Joe Bucciero*
8:15	**Review Project Schedule –** *Philip Huff*
8:40	**Review and Refine CIP-003-5** – Security Management Controls, Change Management, Information Protection and Vulnerability Assessment – *Dave Revill*
10:00	*Break*
10:15	**Review and Refine CIP-004-5 – Personnel and Training –** *Doug Johnson*
12:00	*Lunch*
1:00	**Review and Refine CIP-007-5 and CIP-005-5 – System Security and ESP –** *Jay Cribb*
3:00	*Break*
3:15	**Review and Refine CIP-006-5 – Physical Security–** *Doug Johnson*
5:50	**Review any Drafting Assignments and Thursday's agenda**
6:00	*Recess*

Appendix 1

Project 2008-06 Cyber Security Order 706 SDT
33rd Meeting Agenda
April 12, 2011 Tuesday - 8:00 AM to 6:00 PM PDT
April 13, 2011 Wednesday - 8:00 AM to 6:00 PM PDT
April 14, 2011 Thursday - 8:00 AM to 6:00 PM PDT
Sacramento Municipal Utility District (SMUD)
6201 S Street, Sacramento, CA 95817

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

Proposed Meeting Objectives/Outcomes:

- To review CIP V5 multiple standard format and standard/requirement mapping (CIP-002 – CIP-00X)
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To review and finalize style guide for drafting of CIP requirements
- Initial draft of CIP-002-5 through CIP-009-5 Requirements
- To review and discuss implementation plan concepts
- To agree on next steps and assignments

Thursday April 14, 2011 8:00 a.m. - 6:00 p.m. PDT

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *Philip Huff, Joe Bucciero*
8:15	**Review and Refine CIP-004-5 and CIP-007-5 - Access Control** – *Phil Huff*
10:00	*Break*
10:15	**Review and Refine CIP-008-5 and CIP-009-5 – Incident Response Plan and Recovery Plan –** *Scott Rosenberger*
12:00	*Lunch*
1:00	**Review and Discuss Implementation Plan Concepts –** *Phil Huff*
2:30	**Discussion on Regional Audit staff meeting goals and objectives –** *Phil Huff*
3:00	*Break*
3:15	**Discussion on Regional Audit staff meeting goals and objectives (cont)**
3:45	**Review Communication Plan –** *Joe Bucciero*
4:30	**Review SDT May 2011, Little Rock, AR (AECC) Meeting**
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 1
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
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.	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@kcpl.com
6.	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
7.	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
8.	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
9.	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
10.	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com

APPENDIX 1
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
DRAFTING TEAM ROSTER

11.	Robert Preston Lloyd Sr. Technical Specialist/Scientist	SC&M Technical Support & Strategy Southern California Edison One Innovation Way Pomona, CA 91768	(909) 274-1338 (909) 274-1336Fx robert.lloyd@sce.com
12.	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
13.	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@gatrans.com
14.	Scott Rosenberger Director, Security and Compliance	Luminant 500 North Akard Dallas, Texas 75201	(214) 812-2412 Scott.Rosenberger@ energyfutureholdings.com
15.	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
16.	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
17.	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
18.	John Van Boxtel	Portland General Electric 121 Southwest Salmon Street Portland, Oregon 97204	(503) 464-7093 (503) 317-2464 john.vanboxtel@pgn.com
19.	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
20.	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 1
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
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	Howard Gugel Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 651-2269 howard.gugel@nerc.net
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 2
Meeting Attendees List
April 12-14, 2011 (Sacramento, CA)

Attending in Person — SDT Members and Staff

Name	Company	APR 12	APR-13	APR 14
1. Jay Cribb	Southern Company Services	X	X	X
2. Gerry Freese	AEP	X	X	X
3. Christine Hasha	ERCOT	X	X	X
4. Philip Huff, Vice Chair	Arkansas Electric Coop Corporation	X	X	X
5. Doug Johnson	Exelon Corporation – Commonwealth Edison	X	X	X
6. John Lim, Chair	Consolidated Edison Co. NY	X	X	X
7. Robert Preston Lloyd	Southern California Edison	X	X	X
8. David Revill	Georgia Transmission Corporation	X	X	X
9. Kevin Sherlin	Sacramento Municipal District	X	X	X
10. Tom Stevenson	Constellation	X	X	X
11. Keith Stouffer	National Institute of Standards & Technology	X	X	X
Joe Bucciero	*NERC Facilitator*	*X*	*X*	*X*
Scott Mix	*NERCStaff*	*X*	*X*	*X*
Howard Gugel	*NERC Staff*	*X*		

SDT Members Attending via ReadyTalk and Phone

12. Rob Antonishen	Ontario Power Generation	X	X	X
13. Scott Rosenberger	Luminant Energy	X	X	X
14. John D. Varnell	Tenaska Power Services Co.	X	X	X
15. William Winters	Arizona Public Service, Inc.	X	X	X

SDT Members Not Participating

16. Joe Doetzl	Kansas City Power & Light
17. Sharon Edwards	Duke Energy
18. Bill Gross	NEI
19. Jeff Hoffman	USBR
20. Rich Kinas	Orlando Utilities Corporation
21. John Van Boxtel	Portland General

Appendix 2
Meeting Attendees List
April 12-14, 2011 (Sacramento, CA)

Others Attending In Person or via ReadyTalk and Phone

Matthew Adeleke, Tom Alrich, Jan Bargen, Travis Borrini, John Carpenter, Stephen Carr, Kathy Daggett, David Dockery, Jim Fletcher, Roger Fradenburgh David Gordon, Kuldeep Hak, Michael Keane, Drew Kittey, Kim Koster, Jeff Mantong, Claudine Planter-Pascal, Scott Raymond, Ingrid Rayo,

Appendix 3
Draft Schedule

CSO706 SDT
Meeting Schedule and Objectives (April 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
Little Rock, AR AECC	5/17 to 5/19/2011	Review of Standards and implementation plan

Appendix 3
Draft Schedule

Meeting Location	Dates	Meeting Objective
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 4

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 6
Mapping Document & Framework

CIP-011-1 Numbering	Requirement Description	Proposed CIP-002-5 through CIP-009-5 Numbering	References to Prior Version (Where provided by Subteams)
CIP-011-1 R1	Policy	CIP-003-5 R1	CIP-003-3 R1, R1.1, R1.2, R1.3, R5.1
CIP-011-1 R2	Governance	CIP-003-5 R2	CIP-003-3 R2, R2.2, R2.3
CIP-011-1 R3	Awareness	CIP-004-5 R1	CIP-004-4 R1
CIP-011-1 R4	Training	CIP-004-5 R2	CIP-004-4 R2, R2.1, R2.2.1, R2.2.2, R2.2.3, R2.2.4, R2.3
CIP-011-X R5a	Training - Role Appropriate	CIP-004-5 R3	
CIP-011-1 R5	PRA	CIP-004-5 R4	CIP-004-4 R3, R3.1, R3.3
CIP-011-1 R6	Physical	CIP-006-5 R1	CIP-006-4 R1.1, R1.2, R1.3, R1.5, R4, R4.2, R5, R6
CIP-011-1 R7	Visitors	CIP-006-5 R2	CIP-006-4 R1.6, R1.6.1, R1.6.2
CIP-011-1 R8	Physical Access Control Systems	CIP-006-5 R3	CIP-006-4 R2, R2.1, R2.2, R8, R8.3
CIP-011-1 R9	Access Authorization	CIP-003-5 R5	N/A
CIP-011-1 R10	Account Revocation	CIP-003-5 R6	CIP-004 R4, R4.1, CIP-007 R5, R5.1.3, R5.2
CIP-011-1 R11	Passwords	CIP-007-5 R5	CIP-007 R5.1, R5.2, R5.3
CIP-011-1 R12	Wireless	CIP-005-5 R2	N/A & UA Project 2010-15 (CIP-005 R6)
CIP-011-1 R13	Remote Access Controls	CIP-005-5 R3	N/A & UA Project 2010-15 (CIP-005 R2 & R6)
CIP-011-1 R14	Malicious Code	CIP-007-5 R1	
CIP-011-1 R15	Patch Management	CIP-007-5 R2	CIP-007 R3, R3.1, R3.2
CIP-011-1 R16	Ports & Services	CIP-007-5 R3	CIP-007-4 R2.1, R2.2
CIP-011-1 R17	Security Event Monitoring	CIP-007-5 R4	CIP-005-4 R3, R3.2 CIP-007-4 R6.1, R6.2, R6.3, R6.4, R6.5
CIP-011-1 R18	ESP	CIP-005-5 R1	CIP-005 R1, R2.1, R2.3, R2.6
CIP-011-1	Access Control & Monitoring Systems	CIP-005-5 R4	CIP-005 R1.5
CIP-011-1 R19	Change Management	CIP-003-5 R4	CIP-003-3 R6, CIP-007-3 R1, R9
CIP-011-1 R20	Information Protection	CIP-003-5 R3	CIP-003-3 R4, R4.2, R5, R5.2, R5.3
CIP-011-1 R21	Media Re-Use & Disposal	CIP-007-5 R6	CIP-007-3 R7
CIP-011-1 R22	Maintenance	CIP-007-5 R7	N/A
CIP-011-1 R23	Vulnerability Assessments	CIP-003-5 R7	CIP-005-3 R4.5, CIP-007-3 R8.4
CIP-011-1 R24	Incident Response Plan Specifications	CIP-008-5 R1	CIP-008 R1.1, R1.2
CIP-011-1 R25	Incident Response Plan Testing	CIP-008-5 R2	CIP-008 R1.6
CIP-011-1 R26	Incident Response Plan Review/Communications	CIP-008-5 R3	CIP-008 R1.4, R1.5
CIP-011-1 R27	Recovery Plan Specifications	CIP-009-5 R1	CIP-009 R1.1, R1.2, R4
CIP-011-1 R28	Recovery Plan Testing	CIP-009-5 R2	CIP-009 R2, R5
CIP-011-1 R29	Recovery Plan Review/Communications	CIP-009-5 R3	CIP-009 R1, R5

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.