NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706
32nd Meeting Summary

New York, NY

Tuesday, March 15, 2011 | 8 a.m. to 6 p.m. EDT
Wednesday, March 16, 2011 | 8 a.m. to 6 p.m. EDT
Thursday, March 17, 2011 | 8 a.m. to 6 p.m. EDT

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT- Project 2008-06
32ND MEETING
March 15-17, 2011
New York, NY

Executive Summary

John Lim, Chair of the CSO 706 SDT and host of the meeting welcomed members and other participants to New York and thanked them for their participation in this meeting. John reviewed the meeting location logistics and expressed his thanks to his support team and corporate management in helping to organize the meeting. Howard Gugel, NERC, 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 February 15-17, 2011 Taylor, TX meeting summary. The chair outlined the objectives the SDT sought to accomplish by the end of this meeting that included team review and assessment of CIP Version 5 multiple standard format, finalization of the concepts and number of impact levels that are applicable to these standards, finalization of concepts on the minimum requirements for all BES Cyber Systems, discussion of the drafting the levels of the requirements, reviewing and refining CIP Version 5 BES Cyber System identification and security requirements, and agreement on the team's next steps and assignments. **Appendix 1** contains the meeting agenda.

The Chair reported to that team that two new members of the SDT were approved by the Standards Committee. The new members, Christine Hasha of ERCOT and Robert Lloyd Preston of Southern California Edison, were welcomed to the team, and the Chair expressed his appreciation for their interest and willingness to participate. The team still desires another Canadian representative, which is posted as a vacancy for the team. **Appendix 2** contains the meeting attendance list.

Industry Review:

Scott Mix and John Lim provided an update on other industry activity regarding cyber security. They reported on the discussions held during the recent CIPC meeting including the first cyber attack task force discussions and the scenarios being reviewed across a wide-variety of BES events. Scott reported on the progress of the updates to CIP-005-4 regarding remote access. He reported that revisions were made to the requirements based on industry input and alignment with the CIP reliability standards on cyber security, and the requirements were sent to NERC for posting and ballot. The team is hoping for industry approval. The team for Project 2010-15 is working toward the goal of submitting the approved revised CIP-005-4 to FERC in time for the commission to act in conjunction with the CIP-002-4 action.

Also, DOE and NIST will be working on guidelines or framework for "end-to-end" protection of the grid (generation to distribution). First meeting is scheduled for the end of March 2011 at NIST. An extended group meeting to include more subject matter experts is anticipated for April 2011.

Welcome by Kevin Burke

On Wednesday afternoon, Mr. Kevin Burke, Chairman of the Board and CEO of Consolidated Edison, Inc. and Co-Chair of the EEI CEO Reliability Council addressed the SDT and thanked the team for the work it has done and for its tireless efforts to help the industry achieve secure, reliable operations. He re-enforced the importance of the efforts the drafting team has undertaken and encouraged us to strive forward and achieve our goals to produce a meaningful and technically sound set of reliability standards that address cyber security for the Bulk Electric System.

Needs, Goals, and Objectives:

The SDT reviewed the Needs, Goals, and Objectives document that was developed and adopted at the Columbus meeting, and is provided in **Appendix 3**.

Subteam Assignments

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

Format of CIP Version 5 Standards

The SDT reviewed the format of the next version (Version 5) of the CIP standards as adopted at the Columbus meeting. John Lim created a draft framework for CIP-002-5 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 5** 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 in text boxes for now could eventually 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 volunteered to divide CIP-011 into a proposed CIP-003 to CIP-00x format in time for the next meeting in Sacramento. He asked that the CIP-011 edits being made by the drafting subteams be frozen about a week before the meeting so he can reformat the requirements into CIP-003 to 009.

Impact Levels

The drafting team discussed and considered the number of impact levels that should be included in the CIP standards. The High Impact Level is currently defined today, with all other requirements being in the Low Impact Level. Some of the questions that were addressed are:

- Can we determine the criteria that would cause a requirement to move from a Low Impact Level to a Medium Impact Level (but not a High Impact Level)?
- Do we need a Medium Impact Level?
- What criteria do we use to determine the level of impact (low/medium/high)?
- Is the size of the entity a determining factor?
- What brightline criteria do we use, and are they function-based or asset-based?
- Should the impact levels focus on the individual assets or the impacts on the system for reliability?
- Should devices external to the BES, such as communications devices, be considered?

Phil Huff provided a draft of the scoping criteria for the various impact levels (See **Appendix 6**) for discussion. An Impact Level Subgroup was formed to carry the discussions further and prepare a proposal for the full drafting team to consider. The resolutions proposed by the subgroup were:

a. The new High Impact Level should be higher than the current critical level
b. Definition of BES Cyber System Impact of 15 minutes needs further discussion
c. Other cyber assets considered critical today would be in the new Medium Impact Level
d. Some of the non-critical cyber assets today would also be considered in the new Medium Impact Level (e.g., Assets controlling the ESP could be considered as Medium Impact)
e. Other non-critical cyber assets would be considered in the new Low Impact Level
f. All BES Cyber Systems with only non-routable connections will not require an ESP.
g. Some cyber assets may be considered as non-Impactful.

A graphic was created during the meeting to depict the mapping of the current Critical and Non-Critical Cyber Assets into the proposed High/Medium/Low Impact Levels to be used in Version 5. (See **Appendix 7**)

A straw poll was taken to determine the sentiment of the drafting team regarding the definition of the criteria to be used in determining high/medium/low impact. The criteria voted on were as follows:

High Impact to BES
BES Cyber Systems at Control Centers as specified in **Attachment 1** today (CIP-002-4) with additional controls required by Order 706

Medium Impact to BES
BES Cyber Systems at Field assets (Generation and substations) identified in **Attachment 1** today (CIP-002-4) plus all Control Centers not specified in Attachment 1 (CIP-002-4)
With control levels closer to high than to low, and additional controls required by Order 706 as appropriate

Low Impact to BES
All other BES Cyber Systems not included in Medium or High
With Minimum Control levels (CS Policy, Awareness Program, Electronic Boundary Protections*, Remote Access Controls, Incident Management Program) and additional controls required by Order 706 as appropriate

The results of the straw poll were as follows:
Straw Poll Results: 12 Support 2 Disagree

Those in disagreement want to consider impact classification based on functional impact instead of existing asset-based bright line criteria.

Following the straw poll, a formal vote was taken by the drafting team on this resolution of the impact level definition with the following results:

Formal Vote: 11 Agree 2 Disagree 1 Abstain
Those in disagreement: Rich Kinas and John Van Boxtel
Those abstaining: John Varnell

In addition to the discussion of BES Cyber System impact levels, the team considered adding an additional topical area called Support Systems (e.g., IT Support Services, network services, time synchronization, logging, etc.). John Van Boxtel agreed to help develop the impact level criteria for the IT Support Systems vs. BES Cyber Systems. (See **Appendix 8**)

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. The target is to complete the re-drafting by April 6th, so that the existing CIP-011 requirements can be separated into CIP-003 through CIP-009 before the next drafting team meeting in Sacramento (April 12-14, 2011).

*Note: Cyber Assets that provide Boundary Protection will (may) be protected at a higher level

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

- Mike Keane agreed to try and obtain further clarification regarding defense in depth measures with regard to Boundary Protection in CIP-011 vs. FERC Order 706 P490-505.
- Need a term for "support systems" that will exist within an ESP. Do we need multiple levels of impact defined (high/med/low)?
- Do we need to protect the "support systems" within an ESP at the same level as the ESP?

Drafting Team Schedule

The drafting team reviewed the current project and meeting schedule (See **Appendix 9**), 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.

Meeting Evaluation

The meeting attendees were asked to complete a meeting evaluation. A summary of the results of the responses is provided in **Appendix 10**. These results will be used in planning future meetings of the SDT.

Adjournment

The Chair thanked everyone for attending the meeting, either in person or via the conference call facilities, and expressed his thanks to his Consolidated Edison support team for their assistance.

The meeting adjourned at 3:00 p.m. on Thursday, March 17, 2011

Appendix 1

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EDT
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EDT
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EDT
Con Edison
4 Irving Place, New York, NY 10003

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

Proposed Meeting Objectives/Outcomes:

- To review and assess CIP V5 multiple standard format (CIP-002 – CIP-00X)
- To finalize concepts and number of impact levels
- To finalize concepts on minimum requirements and drafting level of requirements
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Timed Agenda

Tuesday March 15, 2011 8:00 a.m. - 6:00 p.m. EDT

8:00 a.m.	**Introduction, Welcome Opening and Host remarks**- *John Lim, Chair & Phil Huff, Vice Chair,* Roll Call; NERC Antitrust Compliance Guidelines- *Howard Gugel, NERC*
8:15	**Review of meeting objectives and Agenda**- *John Lim*
8:20	**Industry Review**- *Scott Mix, NERC, Mike Keane, FERC and others* o Cyber Attack TF Report o CIPC Report o CIP-005-4 Update o Other Cyber Security business
8:50	**Review of CIP V5 Multiple Standard Format** – *John Lim*
10:00	*Break*
10:15	**Discussion on CIP-002-5 impact levels**
12:00	*Lunch*
1:00	**Discussion on minimum requirements for all BES Cyber Systems**
3:00	*Break*
3:15	**Discussion on level of requirements (high level or detailed/prescriptive, environment, communication protocol)**
5:50	**Review any Drafting Assignments and Wednesday's agenda**
6:00	*Recess*

Appendix 1

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EDT
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EDT
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EDT
Con Edison
4 Irving Place, New York, NY 10003

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

Proposed Meeting Objectives/Outcomes:

- To review and assess CIP V5 multiple standard format (CIP-002 – CIP-00X)
- To finalize concepts and number of impact levels
- To finalize concepts on minimum requirements and drafting level of requirements
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Wednesday February 16, 2011 8:00 a.m. - 6:00 p.m. EDT

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Howard Gugel*
8:15	**Review Project Schedule –** *Philip Huff*
8:40	**Review and Refine BES Cyber System Identification (CIP-002-5)** – *John Lim*
10:00	*Break*
10:15	***Continue,* Review and Refine BES Cyber System Identification**
12:00	*Lunch*
1:00	**Review modifications to style guide for security requirements –** *Philip Huff*
1:30	**Review and Refine CIP-003-5 (Security Policy, Change Management, Information Protection and Maintenance Requirements) –** *Dave Revill, Georgia Transmission*
3:00	*Break*
3:15	***Continue,* Review and Refine CIP-003-5 (Security Policy, Change Management, Information Protection and Maintenance Requirements)**
3:30	**Review and Refine CIP-004-5 (Personnel) and CIP-006-5 (Physical Security Requirements) –** *Doug Johnson, ComEd*
5:50	**Review any Drafting Assignments and Thursday's agenda**
6:00	*Recess*

Appendix 1

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EDT
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EDT
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EDT
Con Edison
4 Irving Place, New York, NY 10003

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

Proposed Meeting Objectives/Outcomes:

- To review and assess CIP V5 multiple standard format (CIP-002 – CIP-00X)
- To finalize concepts and number of impact levels
- To finalize concepts on minimum requirements and drafting level of requirements
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Thursday February 17, 2011 8:00 a.m. - 6:00 p.m. EDT

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Howard Gugel*
8:15	**Review and Refine CIP-004-5 (Electronic Access Control Requirements)** – *Sharon Edwards, Duke Energy*
10:00	*Break*
10:15	**Review and Refine CIP-005-4 and CIP-007-4 (System and Boundary Protection Requirements) –** *Jay Cribb, Southern Company*
12:00	*Lunch*
1:00	**Review and Refine (CIP-008-5) Response and CIP-009-4 (Recovery Requirements) –** *Scott Rosenberger, Future Holdings*
3:00	*Break*
3:15	**Review project schedule and agree to next steps**
4:30	**Review Communication Plan –** *Howard Gugel/Joe Bucciero*
5:00	**Review SDT April 2011 Sacramento, CA (SMUD) Meeting**
6:00	*Adjourn*

Appendix 1

CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM

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 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
Attendees List
March 15-17, 2011 (New York)

Attending in Person — SDT Members and Staff

Name	Company	Mar-15	Mar-16	Mar-17
1. Jay Cribb	Southern Company Services	X	X	X
2. Joe Doetzl	Kansas City Pwr. & Light Co	X	X	X
3 .Sharon Edwards	Duke Energy	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. Rich Kinas	Orlando Utilities Commission	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 Van Boxtel	Portland General	X	X	X
13. William Winters	Arizona Public Service, Inc.	X	X	X
Joe Bucciero	*NERC Facilitator*	*X*	*X*	*X*
Scott Mix	*NERC*	*X*	*X*	*X*
Howard Gugel	*NERC*	*X*	*X*	*X*
Roger Lampila	*NERC*	*X*	*X*	*X*
Brian Harrell	*NERC*		*X*	*X*

SDT Members Attending via ReadyTalk and Phone

14. Rob Antonishen	Ontario Power Generation	X	X	X
15. Jeff Hoffman	USBR	X		
16. Kevin Sherlin	Sacramento Municipal District	X	X	X
17. John D. Varnell	Tenaska Power Services Co.	X	X	X

SDT Members Not Participating

18. Gerry Freese	AEP
19. Bill Gross	NEI
20. Christine Hasha	ERCOT
21. Keith Stouffer	National Institute of Standards & Technology

Appendix 2
Attendees List
March 15-17, 2011 (New York)

Others Attending in Person

Jim Fletcher	American Electric Power
David Dockery	AECI
Martin Narendorf	CenterPoint Energy
Chris Klemm	Encari
Ryan Breed	ERCOT
Mike Keane	FERC
Claudine Planter-Pascal	FERC
Roger Fradenburgh	Network & Security Technologies

Others Attending via Readytalk and Phone

March 15
Matthew Adeleke, Tom Alrich, Stephen Carr, Kathy Daggett, Jay Doran, David Gordon, Drew Kittey, Emily Leone, Andres Lopez, Maggy Powell, Ingrid Rayo, Carrie Reimers, Katie Schnider, Melissa Wehde, Bryn Wilson

March 16
Tom Alrich, Stephen Carr, Kathy Daggett, Jay Doran, David Gordon, Kuldeep Hak, James Julien, Drew Kittey, Patricio Leon-Alvarado, Emily Leone, Andres Lopez, Aileen Meyer, Craig Nelson, Scott Raymond, Ingrid Rayo, Melissa Wehde

March 17
Matthew Adeleke, Tom Alrich, Leo Bernier, Stephen Carr, Kathy Daggett, Jay Doran, David Gordon, Kuldeep Hak, James Julien, Emily Leone, Andres Lopez, Candace Morakinyo, Scott Raymond, Ingrid Rayo, Melissa Wehde

Appendix 3
Needs, Goals and Objectives

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

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.

Appendix 3
Needs, Goals and Objectives

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 complement 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 4
Drafting Subteams

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)*

March 17, 2011

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (March 20, 2008 – April 19, 2008).
2. Revised SAR and response to comments approved by SC (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by NERC Board of Trustees (May 6, 2009).
6. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 3 of CIP-002 to CIP-009 final ballot (December 14, 2009)
8. Version 3 of CIP-002 to CIP-009 approved by NERC Board of Trustees (December 16, 2009)
9. Version 4 of CIP-002 posted for informal comment (December 29, 2009)
10. Version 1 of CIP-010 and CIP-011 posted for informal comment (May 3, 2010)

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 45-day comment period and pre-ballot review.	7/26/2010
2. Conduct initial ballot.	8/30/2010
3. Post response to comments on initial ballot.	9/10/2010
4. Conduct Second Ballot	10/04/2010
5. Post response to comments on second ballot	10/29/2010
6. Conduct Third (recirculation) ballot.	11/08/2010

7. Submit standard to BOT for adoption.	12/10/2010
8. File standard with regulatory authorities.	12/24/2010

Appendix 5

CIP-002-5 – Cyber Security – BES Cyber System Categorization

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Cyber Assets –

Programmable electronic devices including hardware, software, and data in these devices.

BES Cyber System –

One or more Cyber Assets executing or enabling the following BES reliability functions, which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness for the reliable operation of the BES:

One or more Cyber Assets executing or enabling the following BES reliability functions, which if rendered unavailable, degraded, compromised, or misused could restrict control and operation of the BES, or affect situational awareness for the reliable operation of the BES, or, within 15 minutes, cause a Disturbance to the BES:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Control Center –

A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function, or
- Coordination of BES restoration activities.

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

Critical Assets

Critical Cyber Assets

Appendix 5

CIP-002-5 – Cyber Security – BES Cyber System Categorization

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.

4. Applicability:

4.1. Functional Entities:

For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange Coordinator

4.1.4. Transmission Service Provider

4.1.5. Transmission Owner

4.1.6. Transmission Operator

4.1.7. Generator Owner

4.1.8. Generator Operator

4.1.9. Load-Serving Entity

4.1.10. Distribution Provider

4.1.11. NERC

4.1.12. Regional Entity

4.2. The following are exempt from Standard CIP-010-1:

4.2.1. Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3. In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: To be addressed as part of the implementation plan that is currently under development

B. Requirements

R1. Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in *CIP-002 – 5 Attachment I – Functions Essential to the Reliable Operation of the BES* , and the functions it executes or enable, to identify BES Cyber Systems for the application of security requirements. *(Violation Risk Factor: High)*

Measure M1. The Responsible Entity shall have evidence identifying and documenting each of its BES Cyber Systems that execute or enable 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.

R2. Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in *CIP-002-5 Attachment II – Impact Categorization of BES Cyber Systems* to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES. *(Violation Risk Factor: High)*

Measure M2. The Responsible Entity shall have evidence identifying the categorization of each of its BES Cyber Systems that execute or enable functions defined in *CIP-002 – 5 Attachment I – Functions Essential to the Reliable Operation of the BES* categorized in accordance with *CIP-002 – 5 Attachment II – Impact Categorization of BES Cyber Systems* as required in R2.

R3. To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall: *(Violation Risk Factor: High)*

- **3.1.** review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization
- **3.2.** review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns
- **3.3.** update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES.

Measure M3. The Responsible Entity shall have evidence that it has reviewed its identification and categorization of its BES Cyber Systems and updated the applicable documentation within 45 calendar days of the completion of the review or the completion of such change to the BES.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Data Retention

Each Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence for Requirements R1, R2 and R3, and Measures M1, M2 and M3 for a full calendar year or since the last audit, whichever is longer.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority, in conjunction with the Registered Entity, shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits
Self-Certifications

Spot Checking
Compliance Violation Investigations
Self-Reporting
Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
1	5% or fewer BES Cyber Systems have not been identified.	More than 5% but less than or equal to 10% of BES Cyber Systems have not been identified.	More than 10% but less than or equal to 15% of BES Cyber Systems have not been identified.	More than 15% of BES Cyber Systems have not been identified.
2	5% or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 5% but less than or equal to 10% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 10% but less than or equal to 15% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 15% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.
3	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 45, but less than or equal to 60 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 60, but less than or equal to 70 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 70, but less than or equal to 80 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 80 calendar days following the completion of the change.

D. Regional Variances

None.

VERSION HISTORY

Version	Date	Action	Change Tracking
1.000	5/3/2010	Initial draft of Version 1 posted for informal comment.	

CIP-002-5 Attachment I

Functions Essential to Reliable Operation of the Bulk Electric System

The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes.

Dynamic Response - Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Balancing Load and Generation - Activities, actions and conditions for monitoring and controlling generation and load.

Controlling Frequency (Real Power) - Activities, actions and conditions to control frequency within defined bounds.

Controlling Voltage (Reactive Power) - Activities, actions and conditions to control voltage within defined bounds.

Managing Constraints - Activities, actions and conditions to maintain operation of BES elements within their design limits and constraints.

Monitoring & Control - Activities, actions and conditions that provide monitoring and control of BES elements.

Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Situational Awareness - Activities, actions and conditions to assess the current, expected, and anticipated state of the BES.

Inter-Entity Real-Time Coordination and Communication - Activities, actions and conditions for real-time coordination and communication between Responsible Entities' System Operators.

CIP-002-5 - Attachment II

IMPACT CATEGORIZATION OF BES CYBER SYSTEMS

1. High Impact Rating (H)

Each BES Cyber System that can affect operations for:

1.1. An aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

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

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

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

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

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

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

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

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

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

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

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

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

2. Medium Impact Rating (M)

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

3. Low Impact Rating (L)

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

Appendix 6
Proposed Impact Levels
March 15-17, 2011 (New York)

Impact Level	*High*
Objective: Protect those Cyber Assets that could be a specific target of BES reliability	
Scoping Criteria: based on Attachment I in CIP-002-4 using functions essential to the BES (Attachment II in CIP-002-5 using Attachment I for function identification)	

Impact Level	*Medium?*
Objective	
Scoping Criteria: Cyber Assets that used to support functions that are required for other NERC reliability standard obligations. (RC,TOP,BA)	

Impact Level	*Low*
Objective : Protect those Cyber Assets that attackers can use as a launching point to high impact assets or attackers can potentially gain access to a large number of facilities	
Scoping Criteria: Those individual Cyber Assets that are associated with BES facilities that have an impact on real time operations, but individually have an impact that can be controlled through existing processes or plans or immediate mitigation action is not required.	
Option 2: Those BES Cyber Systems, not identified as High or Medium Impact BES Cyber Systems, that individually if destroyed, degraded, misused or otherwise rendered unavailable do not have an impact to a BES Function beyond those identified in other NERC standard requirements.	

Impact level is the impact on the BES given a particular entity performing a particular function in Attachment I.

Appendix 6
Proposed Impact Levels
March 15-17, 2011 (New York)

Impact level is the impact on the BES of a particular BES Cyber System's performance of a function in Attachment I, if it is destroyed, degraded, misused or otherwise rendered unavailable.

Impact level is impact to the BES by a BES Cyber System.

Appendix 6
Proposed Impact Levels
March 15-17, 2011 (New York)

Applicability (From CIP Cyber Security Standards Style Guide – January)

The applicability section should be used, where appropriate, for the following types of exceptions.

- ***Impact Level and Operating Environment*** – Specify whether this security requirement applies to all identified BES Cyber Systems or only Impact Level A or B. A description of each impact level is described below:

BES Cyber Systems at Transmission Facilities

Characterized by long stretches of geographical separation between sites. Hard to physically defend economically.

- **Impact Level B BES Cyber Systems**
  Primary Concern: Attackers using it as a launching point to high impact assets or attackers gaining easy access to a large number of facilities.
  - Controlled access to upstream networks (limit use as a launching point for attacks)
  - All passwords must be changed from manufacturer defaults on all devices that support a password.
  - Strong authentication required for all remote electronic access
  - Good ingress & egress network access control
  - No physical security requirements
  - General Organizational Controls
- **Enhancements for Impact Level A BES Cyber Systems**
  Primary Concern: The Cyber System is itself a target.
  - Physical access control and logging.
  - Electronic access control and logging for all remote access.
  - Little to no systems management in substation environment since it consists mostly of dedicated devices (IEDs). Make it mostly about strong access control both electronically and physically with notifications of unauthorized access.

BES Cyber Systems at Generation Facilities

Campus with widely distributed cyber components. Longer system lifecycle and challenging test environment.

- **Impact Level B BES Cyber Systems**
  Primary Concern: Attackers using it as a launching point to high impact assets or attackers gaining easy access to a large number of facilities.
  - Controlled access to upstream networks (limit use as a launching point for attacks)

- All passwords must be changed from manufacturer defaults on all devices that support a password.
- Strong authentication required for all remote electronic access
- Good ingress & egress network access control
- No physical security requirements
- Organizational Controls

- **Enhancements for Impact Level A BES Cyber Systems**
  Primary Concern: Attackers gaining control of single large units or multiple units within the plant.
  - Physical access control and logging.
  - Strong, highly controlled segmentation between individual generating units.
  - Electronic access control and logging for all remote access.
  - Good systems management, change mgt, vulnerability mgt on control system servers, HMIs.

BES Cyber Systems at Control Centers
Centralized data centers. Easier to apply automated security controls.

- **Impact Level B BES Cyber Systems**
  Primary Concern: Attacks over their connectivity to higher impact control centers
  - Controlled access to other control networks.
  - Strong authentication required for all remote electronic access
  - Controlled physical access.
  - Vulnerability management on all connected systems
- **Enhancements for Impact Level A BES Cyber Systems**
  Primary Concern: The ultimate target – gaining control of numerous assets.
  - All the current requirements plus Order 706 changes plus what makes sense out of 800-53.
  - The strongest perimeters (physical and electronic)
  - Stringent systems management, change mgt, vulnerability mgt.
  - Strong personnel controls.

Appendix 7
Proposed Impact Levels
March 15-17, 2011 (New York)

NERC CIP IMPACT LEVELS PROPOSAL

The SDT begins drafting according to the following concepts regarding impact levels and general applicability of security controls:

High Impact to BES
BES Cyber Systems at Control Centers as specified in Attachment 1 today (CIP-002-4) with additional controls required by Order 706

Med Impact to BES
BES Cyber Systems at Field assets (Generation and substations) identified in Attachment 1 today (CIP-002-4) plus all Control Centers not specified in Attachment 1 (CIP-002-4)
With control levels closer to high than to low, and additional controls required by Order 706 as appropriate

Low Impact to BES
all other BES Cyber Systems not included in Med or High
With Minimum Control levels (CS Policy, Awareness Program, Electronic Boundary Protections*, Remote Access Controls, Incident Management Program) and additional controls required by Order 706 as appropriate

All BES Cyber Systems with only non-routable connections will not require an ESP.

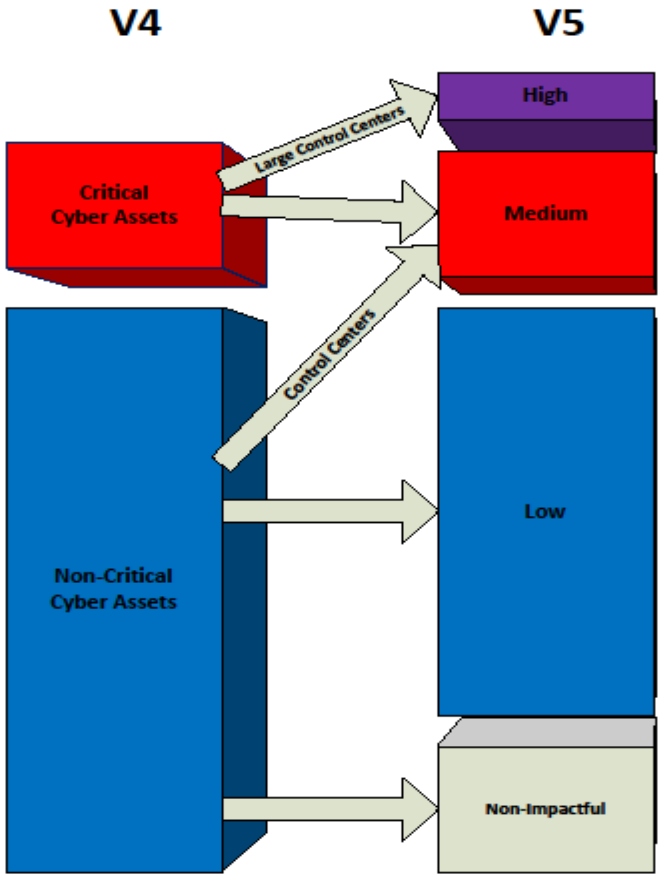
*Devices that provide Boundary Protection will (may) be protected at a higher level.

Straw poll - 12 Support 2 Disagree

Disagreement involved impact classification should be function based instead of existing asset based bright line criteria.

Formal vote: 11 Agree 2 Disagree 1 Abstain

Appendix 7
Proposed Impact Levels
March 15-17, 2011 (New York)



Drawing not to scale

Appendix 8
Groups of Cyber Assets
March 15-17, 2011 (New York)

Groups of Cyber Assets (Systems):

1. BES Cyber Assets (H/M/L)
   Collection of BES Cyber Assets is a BES Cyber System

2. Other (Logically Associated Devices) Protected Cyber Assets within the ESP (H/M)
3. Protective Assets (Systems)
   a. Logical Access Control Systems (Firewalls, external interactive devices, …)
   b. Physical Access Control Systems – control, monitoring, logging of physical access (Card access systems, …)
   c. Monitoring Protective Systems (Log aggregation, monitoring, …)
4. Support Systems
   a. Logical Support Cyber Assets (DNS, SAN, Virtualization, …)
   b. Physical Support Cyber Assets (UPS, HVAC, …)
5.

Appendix 9
CSO706 SDT Meeting Schedule
March 15-17, 2011 (New York)

(March 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 9
CSO706 SDT Meeting Schedule
March 15-17, 2011 (New York)

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
Baltimore, MD Constellation	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 10
CSO706 SDT Meeting Schedule
March 15-17, 2011 (New York)

Question 1
How would you rate the overall meeting in accomplishing the necessary objectives?

Average	3.6/4
Comments	difficult topic acceptable progress

Question 2
How would you rate the effectiveness of the full team in this meeting?

Average	3.6/4
Comments	the process although slow produces results that can pass a ballot

Question 3
How would you rate the effectiveness of the chair/vice chair?

Average	4/4
Comments	Their leadership promotes the free exchange of ideas. And, provides the opportunity to reexamine past decisions to produce solid results

Question 4
How would you rate the effectiveness of distributed agenda and meeting materials prior to this meeting?

Average	3.5/4
Comments	The calendar sent by Howard on 3/9 was the old one w/ posting of V5 by this June. would be great to have in one email as early as possible

Question 5
How would you rate the use of visual and audio aides for this meeting?

Average	3.5/4
Comments	Much better sound than previous meetings! as discussed in last meeting's evaluation... The single monitor approach makes it difficult for the NERC staff to manage the requests for displaying files in a timely manner Need more mics and mute the calls so we can't hear people cooking and cursing :-)

Question 6
How would you rate the use of sub-team meetings in between face-to-face meetings

Average	3.1/4
Comments	this facilitates progress in the full team meetings More participation is desired. We need to make sure that the leaders are clear on the guidelines that were agreed to and have a clear understanding of what needs to be accomplished between meetings. Style Guide, Impact levels, Applicability

Question 7
Please provide other suggested improvements or any other general comments.

Comments	You're doing a great job! I am grateful to the entire team for granting me the opportunity to participate. It has improved our CIP program at home. no vomet flavored jelly beans provided Good to be back

Since the most important item is probably going through the requirements, I think we need to move that item up on the agenda. It seems we never begin that process until near the last day of the meetings. So, we always run out of time. This needs to be avoided.
Also, we somehow need to limit the discussion to relevant recommendations for improvements in the language of the requirement. I thought the Access Control review did not go too well because we spent the first 2 hours arguing whether entities need to identify the types of accounts they have or not. The teams were told to review the DHS catalog and incorporate requirements where it seemed appropriate. I suspect that some on the team will be suspect of any requirement that does not look like it came from CIP v1-3. Perhaps we need to re-visit the direction of incorporating DHS requirements if this type of push back continues.