Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EST
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EST
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EST
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. EST

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*

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EST
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EST
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EST
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. EST

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*

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EST
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EST
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EST
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. CST

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*

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

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
Vice Chairman	Philip Huff Security Analyst	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
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
	Jim Brenton, CISSP-ISSAP Principal, Regional Security Coordinator	Electric Reliability Council of Texas, Inc. 2705 WCST Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ ercot.com
	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
	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@ kcpl.com
	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
	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
	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
	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com

	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@ gatrans.com
	Scott Rosenberger Director, Security and Compliance	Luminant 500 North Akard Dallas, Texas 75201	(214) 812-2412 Scott.Rosenberger@ energyfutureholdings.com
	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
	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
	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
	John Van Boxtel	Portland General Electric 121 SouthwCST Salmon Street Portland, Oregon 97204	(503) 464-7093 (503) 317-2464 john.vanboxtel@pgn.com
	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
	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
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

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

CSO706 SDT
Meeting Schedule and Objectives

Meeting Location	Dates	Meeting Objective
Columbus, OH AEP	01/18 to 01/20/2011	Full review of CIP-011 requirements in response to industry comment (first of several development iterations for posting in late June)
Interim	1/20 to 2/15/2011	Designated individuals complete drafting assignments on CIP-011
Taylor, TX ERCOT	2/15 to 2/17/2011	Begin review of CIP-010, BES Cyber System Identification Full review of CIP-011 (requirements, measures, change rationale, guidance)
Interim	2/17 to 3/15/2011	Designated individuals complete drafting assignments on CIP-010 and CIP-011 Begin developing implementation plan
New York, NY ConEd	3/15 to 3/17/2011	Review of CIP V5 (requirements, measures, change rationale, guidance) Initial review of implementation plan
Interim	3/17 to 4/12/2011	Designated individuals complete drafting assignments on CIP V5 and implementation plan
Sacramento, CA SMUD	4/12 to 4/14/2011	Review of CIP V5 and implementation plan
Interim	4/14 to 5/17/2011	Designated individuals complete drafting assignments on CIP V5 and implementation plan Sneak peak industry webinar in early May
Little Rock, AR AECC	5/17 to 5/19/2011	Review of industry feedback Review of change rationale and guidance
Interim	5/19 to 6/21/2010	Designated individuals complete drafting assignments on CIP V5 and implementation plan NERC begins QA

Meeting Location	Dates	Meeting Objective
????????	6/21 to 6/23/2011	SDT and NERC QA on document for posting
Interim	6/23 to 7/19/2011	Posting for comment Prepare for technical workshop?
TBD	7/19 to 7/21/2011	Technical Workshop?
TBD	8/23 to 8/25/2011	Respond to comments
TBD	9/20 to 9/22/2011	Respond to comments and prepare for second posting and ballot
TBD	10/11 to 10/13	

CSO 706 SDT DRAFTING SUB-TEAMS

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton *(Observer Participants: Rod Hardiman, Jim Fletcher, Dave Burtrum)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
Framework CIP 010 &011	Jay Cribb (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Norton, Dave Revill, Jon Stanford and John Van Boxtel. Mike Keane FERC and Scott Mix, NERC

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.

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.

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.