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

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

Proposed Meeting Objectives/Outcomes:

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

Timed Agenda

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

8:00 a.m.	**Introduction, Welcome Opening and Host remarks**- *John Lim, Chair & Phil Huff, Vice Chair, David Dockery, AECI* Roll Call; NERC Antitrust Compliance Guidelines- *Joe Bucciero, NERC*
8:15	**Review of Meeting Objectives, Agenda and Procedures** - *John Lim*
8:45	**Industry Updates** - *Scott Mix, NERC, Mike Keane, FERC and others* o Cyber Attack TF Report o DOE/NIST/NERC Risk Management Process o CIP-005-4 Update o Other Cyber Security business
9:30	**Overview of CIP Version 5 development and progress –** *John Lim*
10:00	*Break*
10:15	**Overview of Issues Found through CIP Audits –** *Roger Lampila/Tom Hofstetter*
11:00	**BES Cyber System Definitions –** *John Lim*
12:00	*Lunch*
1:00	**BES Cyber System Definitions (cont.) –** *John Lim*
2:00	**CIP-002-5 BES Cyber System Identification Requirements –** *John Lim*
3:00	*Break*
3:15	**CIP-002-5 BES Cyber System Identification Attachment 1 Criteria** - *John Lim*
4:30	**CIP-003-5 Governance Requirements (2) –** *Dave Revill, Georgia Transmission*
5:30	*Recess*

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

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

Proposed Meeting Objectives/Outcomes:

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

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

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

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

10:20 *Break*

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

11:45 *Lunch*

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

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

3:05 *Break*

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

5:30 *Recess*

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

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

Proposed Meeting Objectives/Outcomes:

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

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

8:00 a.m. **Recap of Day 2, Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Joe Bucciero*

8:15 **CIP-007-5 Systems Security Requirements (5) –** *Phil Huff, AECC*
- *R5 – System Access Controls*

8:55 **CIP-008-5 Incident Response Requirements (3) –** *Scott Rosenberger, Energy Future Holdings*
- *R3 – Incident Response Plan Review, Update, Communicate*

9:35 **CIP-009-5 Recovery Plans (3) –** *Scott Rosenberger, Energy Future Holdings*
- *R1 – Recovery Plan Specifications*

10:15 *Break*

10:35 **CIP-009-5 Recovery Plans (2) –** *Scott Rosenberger, Energy Future Holdings*
- *R2 – Recovery Plan Testing Specifications*
- *R3 – Recovery Plan Review, Update, Communicate*

11:45 *Lunch*

12:45 **CIP-010-5 Change Management Requirements (3) –** *Dave Revill, Georgia Transmission*
- *R1 – Configuration Change Management*
- *R2 – Configuration Monitoring*
- *R3 – Vulnerability Assessments*

2:20 **CIP-011-5 Information Protection Requirements (2) –** *Dave Revill, Georgia Transmission*
- *R1 – Information Protection*
- *R2 – Media Reuse and Disposal*

3:15 *Break*

3:30 **Remote Access Urgent Action CIP-005-4 Revisions –** *Christine Hasha, ERCOT*

3:45 **Open Discussion of Version 5 CIP-002 through CIP-011 Standards**
- *Review Outstanding Issues & Items*
- *Wrap-Up*

4:45 **SDT Review of July Meeting Agenda and Next Steps**

5:00 **SDT Establish Subteam Meeting Schedule**

5:30 *Adjourn*

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

Format of Requirements Discussion for CIP-003 through CIP-011 Requirements

The review of each requirement in CIP-003 through 011 will follow a strict time format as shown below. This is to ensure we have enough time in the three day meeting to review all requirements. The definitions and CIP-002 discussion will follow a slightly different format and displayed during the meeting.

*Regional audit persons have precedence in the review of the Standard. Please **raise your tent cards** to get in the queue each time we transfer to a new requirement. **The number of times a person has commented may affect their placement in the queue**. For open discussion, all persons attending the meeting and on the phone may raise their cards/hands to join the queue. The SDT panel will be given a chance to respond for each comment.*

There will be a short amount of time at the end of the three day meeting to further discuss issues. Also, please make use of the breaks to continue discussions.

Longer Timed Requirements (i.e. Personnel Risk Assessment) – Total 40 minutes each
1. Regional Auditor #1 poses question or comments (3 minutes)
2. SDT Member Forum Response (2 minutes)
3. Regional Auditor #2 poses question or comments (3 minutes)
4. SDT Member Forum Response (2 minutes)
5. Regional Auditor #3 poses question or comments (3 minutes)
6. SDT Member Forum Response (2 minutes)
7. Regional Auditor #4 poses question or comments (3 minutes)
8. SDT Member Forum Response (2 minutes)
9. Open discussion (20 minutes)

Medium Timed Requirements (i.e. Access Revocation) – Total 30 minutes each
1. Regional Auditor #1 poses question or comments (3 minutes)
2. SDT Member Forum Response (2 minutes)
3. Regional Auditor #2 poses question or comments (3 minutes)
4. SDT Member Forum Response (2 minutes)
5. Regional Auditor #3 poses question or comments (3 minutes)
6. SDT Member Forum Response (2 minutes)
7. Open discussion (15 minutes)

Shorter Timed Requirements (i.e. Security Awareness) – Total 15 minutes each
1. Regional Auditor #1 poses question or comments (3 minutes)
2. SDT Member Forum Response (2 minutes)
3. Regional Auditor #2 poses question or comments (3 minutes)
4. SDT Member Forum Response (2 minutes)
5. Open discussion (5 minutes)

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

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

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

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

CSO706 SDT
DRAFT Meeting Schedule and Objectives

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 5/16/2011	Sub-teams continue drafting requirements.
Little Rock, AR AECC	5/17 to 5/19/2011	Review of Standards and Communications plan Prepare for June Meeting with NERC Regional Compliance/Audit Staff
Interim	5/20 to 6/3/2010	Sub-teams finalize requirements drafts, and prepare for issue to NERC & Regional Compliance/Audit Staff
Interim	6/4 to 6/20/2011	Sub-teams prepare comment response summaries from CIP-010 and 011 informal posting in 2010. Begin preparation of Implementation Plan and Guidelines Documentation

CSO706 SDT
DRAFT Meeting Schedule and Objectives

Meeting Location	Dates	Meeting Objective
Springfield, MO AECI	6/21 to 6/23/2011	Review of Standards with NERC and Regional Compliance/Audit Staff
Interim	6/24 to 7/18/2011	Sub-teams continue drafting requirements based on feedback from NERC and Regional Compliance/Audit Staff. Continue preparation of Implementation Plan and Guidelines Documentation Prepare mapping document from CIP V4 to V5 Members to update their representative Industry stakeholder organizations on the V5 requirements
Salt Lake City, UT WECC	7/19 to 7/21/2011	Walk-through sample generation and substation environments with the Version 5 requirements to determine feasibility. Output additional guidance based on the walk-through process
Interim	7/22 to 8/15/2011	Sub-teams revise drafting requirements based on feedback from walk-through process Prepare for August Meeting with representatives from Industry stakeholder organizations
Washington, DC	7/28/2011	Drafting Team Meeting with FERC Staff
Atlanta, GA NERC	8/16 to 8/18/2011	Review of Standards with Industry Representatives
Interim	8/19 to 9/19/2011	Sub-teams revise drafting requirements based on feedback from Industry Representatives CSO706 Drafting Team begins preparation of all documentation for submittal to NERC Quality Review
WEBINAR	8/24/2011	Industry Webinar as outreach to present concepts and schedule for Version 5 CIP Standards
Orange County, CA SCE	9/20 to 9/22/2011	CSO706 Drafting Team finalizes CIP Standards, implementation plan, and other documentation for NERC Quality Review

CSO706 SDT
DRAFT Meeting Schedule and Objectives

Meeting Location	Dates	Meeting Objective
Quality Review	9/23 to 10/7/2011	NERC Quality Review & meeting with DT leadership and subteam leads to provide comments
Interim	10/8 to 10/24/2011	Subteams to update standards and all documentation based on QR and prepare for posting
Constellation Baltimore, MD	10/25 to 10/27/2011	SDT Meeting to consider QR changes made to the standards and finalize standards for posting
Interim	10/28 to 11/3/2011	Review Response to Suggested Changes with QR Team
POSTING	11/3/2011	Post CIP Standards for 45+ day formal comment with concurrent ballot
Comment & Ballot	11/4 to 12/19/2011	Version 5 CIP Standards 45+ day formal Comment and Ballot Period
WEBINAR	11/15/2011	Industry Webinar as outreach to present concepts and schedule for Version 5 CIP-002 through CIP-005 Standards
WEBINAR	11/29/2011	Industry Webinar as outreach to present concepts and schedule for Version 5 CIP-006 through CIP-011 Standards
OUC/FRCC Orlando/Tampa, FL	11/29 to 12/1/2011	Drafting Team Meeting to consider Webinar input and to prepare for formal comments and concurrent ballot comments
Review Comments	12/20/2011 to 1/23/2012	Review formal comments and concurrent ballot comments and prepare responses Revise standards for re-posting for 30-day comment and ballot
Location (??)	1/24 to 1/26/2012	Drafting Team Meeting to finalize responses to formal comments and finalize documents for 30-day comments and ballot posting
Quality Review	1/27 to 2/10/2012	NERC Quality Review & meeting with DT leadership and subteam leads to provide comments

CSO706 SDT
DRAFT Meeting Schedule and Objectives

Meeting Location	Dates	Meeting Objective
Interim	2/13 to 2/17/2012	Subteams to update standards and all documentation based on QR and prepare for posting
Location (??)	2/21 to 2/23/2012	SDT Meeting to consider QR changes made to the standards and finalize standards for successive ballot posting
POST Responses to Comments	2/24/2012	Post responses to 45-day formal comments and ballot comments
Comment & Ballot	2/24 to 3/26/2012	30-day Posting for comment and successive ballot
Interim	2/24 to 3/19/2012	Begin preparation of FERC filing documentation
Location (??)	3/20 to 3/22/2012	Drafting Team Meeting to prepare for 30-day formal comments and successive ballot comments
Interim	3/23 to 4/23/2012	Continue preparation of FERC filing documentation Subteam meetings to prepare responses to successive ballot comments and revise Standards, as necessary
Location (??)	4/24 to 4/26/2012	Drafting Team Meeting to finalize responses to comments and prepare revisions to Standards for recirculation ballot
Post for Ballot	4/30/2012	Post for recirculation ballot
Interim	4/30/2012 5/11/2012	Recirculation Ballot
Finalize standards	5/12 to 5/31/2012	Finalize CIP standards text for filing

Schedule, meetings, postings, and ballots will be reviewed @ June 2011 meeting.

Other host options:

Arizona Public Service	ComEd
ERCOT	Georgia Transmission
Ontario Power Generation	SERC
Southern California Edison	Southern Co

CSO 706 SDT DRAFTING SUB-TEAMS
VERSION 5

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

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.