NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706 Meeting Summary with FERC Technical Staff

FERC's Offices
Washington, DC

Thursday, July 28, 2011 |9 a.m. to 5 p.m. EDT

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT-Project 2008-06
Meeting with FERC Technical Staff
July 28, 2011
Washington, DC

Meeting Summary

John Lim, Chair of the CSO 706 SDT welcomed members, FERC's Technical Staff, and other participants to this meeting of the CSO 706 SDT with FERC Technical Staff, and he thanked everyone for their participation in this meeting. John also acknowledged and thanked Jan Bargen and Michael Keane for all of their efforts in making the meeting possible. Jan Bargen reviewed the meeting logistics and safety information. At the beginning of the meeting, Joe Bucciero, NERC Facilitator, conducted a roll call, reviewed the public meeting notices, and presented the NERC antitrust guidelines.

The Chair outlined the meeting objectives, which included a brief status review of CIP Version 5 Standards Development and the project schedule, open dialogue with FERC Technical Staff concerning any issues they may have with regard to the current draft of the CIP Version 5 standards, discussion of the drafting team's questions of FERC's Technical Staff, and identification of any potential questions and issues that may require further review and discussion within the drafting team during future drafting team meetings. **Appendix 1** contains the meeting agenda.

Appendix 2 contains the meeting attendance list, and the current drafting team roster is included in **Appendix 3**.

Status Review of CIP Version 5

John Lim, Chair, briefly reviewed the principles that were established and are being followed by the drafting team in updating the CIP Reliability Standards on cyber security **(Appendix 5)**, and he provided a brief overview presentation concerning the CIP Standards and Concepts being implemented in Version 5 of the CIP Reliability Standards on Cyber Security. **Appendix 7** contains a hotlink to a copy of the presentation.

Drafting Team Schedule

Phil Huff, Vice-Chair, reviewed the current project and meeting schedule (**Appendix 4**), including the upcoming meeting dates, objectives, and locations. Phil confirmed that the August 2011 meeting of the drafting team (August 16-18, 2011) will be an open session with representatives from industry stakeholder organizations in Atlanta, GA, at NERC's new headquarters facilities to review the current draft of Version 5 of the CIP Cyber Security Standards. This meeting is part of the continuing outreach effort adopted by the drafting team to meet with various organizations within the industry to help clarify and explain the requirements included in the current draft of the Version 5 CIP Standards.

The drafting team has already met with members of the NERC regional compliance organizations, and plans to meet with the industry stakeholder organizations subsequent to this meeting with FERC staff.

A series of Webinars is also planned to help inform the industry participants of the requirements included in Version 5 of the CIP Standards. The next webinar is scheduled for August 24, 2011.

FERC Technical Staff Questions of the Drafting Team

The FERC Technical Staff addressed a variety of topics through their questions and comments to the CSO706 standard drafting team. The FERC Technical Staff stated that it does not speak for the Commission or the Commissioners, and that their questions are being addressed to the drafting team with the intention of gaining some additional clarity and insight into the topical areas.

General Comments

The initial general comments from FERC Technical Staff indicated that they were pleased with the previous face-to-face meeting with the drafting team that occurred in May 2010, and were looking forward to the same types of results from this meeting. Staff was encouraged by the inclusion of additional industry webinars in the drafting team's schedule that included time for industry feedback and comment. The SDT was asked to consider scheduling a pre-filing meeting with FERC Technical Staff, similar in agenda and design to the current meeting.

FERC Technical Staff expressed their appreciation for the apparent FISMA influences in the approach to the Version 5 standards that provide more attention to the identification of cyber assets and cyber systems that are needed for an entity to perform its functional obligations to BES reliability (instead of the initial focus on critical equipment assets). All cyber assets should have some degree of cyber security protection, while those cyber asset having greater reliability impacts would require additional protections.

Scope and Levels of Protection

This concept of protection led to additional discussion of the bright line criteria included in the CIP-002 standard, and in particular, what was the rationale for selecting the existing bright lines that resulted in the High, Medium, and Low impact levels? Is the three tier classification correct? Are enough assets and systems protected at the right levels to provide security from aggregated (vs. the one off) attacks? Staff expressed concern that this type of attack requires more of a "system and software engineering" approach instead of the more traditional "power engineering" approach. Staff remains concerned that the proposed standards have not yet achieved this goal (e.g., there seemed to still be a very strong emphasis on "big iron" electrical assets versus systems and functionality).

FERC Staff expressed concern that the scope of assets identified for protection should include the specific cyber computing, networking connectivity, data, and associated computing infrastructure assets used in the execution of the cyber-based systems applications an entity relies upon to conduct its registered functions.

Staff asked if there were any new security controls (e.g., encryption, cryptographic integrity checks, etc) identified to protect the High impact level asset, inquiring about incorporating an intrusion monitoring requirement, as an example. NERC staff stated that the use of encryption would compromise availability of the data/system. FERC Staff was also concerned whether there are sufficient security controls within the Low impact level and medium impact level to adequately protect the cyber assets in those categories (e.g., does each impact level have the appropriate and sufficient security controls). Should additional controls be borrowed from NIST and adapted to this model? This scoping issue is to some extent two phased: Are the right cyber assets categorized in the right impact level categories, and does each impact level category have the right security controls that will be used to protect those systems in that category?

The drafting team responded that a lot of thought and engineering went into selecting the bright-line criteria, and, in contrast to FERC Staff's concern, it believes that the criteria used are justified and adequate. The bright line criteria in Version 5 does address the additional impact classification levels vs. Version 4, and is directed more to the cyber asset and system asset.

FERC Staff reminded the team that "data" should also be considered as a "cyber asset" as stated in 706. The SDT should consider the need for the definition of a "data center" that is not co-located with the control center. How should these facilities be considered regarding their impact levels on reliability operation of the grid? Environmental, communications capability, and connectivity concerns should also be considered in the criteria definition. Perhaps the concept of connectivity and its impact on the applicability of the requirements need additional explanation. The drafting team indicated that defense in depth is being applied at the perimeter of all control and data centers, but further discussion is needed. The SDT discussed the need to revisit the concept of the "physical access control system".

Timeframes for Actions

FERC Staff expressed concern that some of the timeframes for action in the requirements seem too open-ended. The drafting team should consider further discussions to try and tighten-up the required timeframes for action and provide some form of explanation or justification for when choosing not to do so. Staff requested an explanation of the meaning and thoughts behind the "impact with 15-minutes" criterion. What is meant by the 15-minute timeframe? How is it measured? Staff stated that the definition of 15-minute timeframe in this context is required or at the least included as a footnote. Staff opinioned that a full explanation in the guidance documents is inadequate, since guidance documents are not enforceable.

Of additional concern is whether the 15 minute clock consideration starts from the initiation of the attack or upon the discovery. The SDT indicated that the 15 minutes is from the loss of the system (e.g., start of attack) and until the impacts are felt by operations. FERC staff is not convinced that 15 minutes is the proper delimiter and suggested that, if a system is lost and the impact would be felt within 30, or perhaps 60 minutes, it should be within scope to be protected to ensure that systems important to the grid are captured. The group discussed various ramifications in the context of the SDT's example of a coal bunker refill system where, if the bunker was full before the attack, there would be approximately 8 hours or more reserve before it's loss would be felt by the generator. FERC staff asked whether all systems functionally important from a regional perspective will be captured under the proposal.

Policy/Plan/Procedures/Program

FERC Staff stated that requirements revolving around policy, plan, procedure, and program need further explanation regarding what is intended and what measures should be used to gauge compliance. The drafting team should consider including identification of the topics to cover as part of the policy, plan, procedure, or program requirements and possibly add those in the measures. Should a minimum set of topics be included in the requirement statement, while the guidance can expand on the examples? Should these terms be defined, since they have different connotations across the disciplines that work together to implement the standards?

Connectivity vs. Requirement Applicability Threshold

FERC Staff expressed concern that, in Version 4, cyber assets were considered either critical or non-critical, but may now be split between Medium and High Impact. The drafting team indicated that the intent in Version 5 is to provide equivalent or greater controls on those assets, and the Medium and High categorizations are intended to provide that distinction. The applicability portion of the requirements is based on both the categorization and connectivity of the cyber asset, and the drafting team will further explain this in the guidance document.

VRF/VSL Definitions

FERC Staff reminded the drafting team that the VRF/VSL designations may not correlate directly to the Version 4s, given the paradigm shift that Version 5 is attempting. Furthermore, the new procedures submitted for approval last year and recently approved by the Commission should be used when evaluating whether or not all components of a requirement can be addressed by one VRF/VSL, and whether or not the VSL can be gradated. The drafting team will verify that any paradigm shifts the requirements from Version 4 to Version 5 will be considered when developing the VRF/VSLs for the Version 5 CIP Standards.

Implementation Plan

FERC Technical Staff encouraged the drafting team to develop the implementation plans for Version 5 CIP standards independently of the Version 4 timelines, and to be creative across categories to move implementation forward as readily as possible across the board. The Version 5 Implementation Plan should assign short-term implementations where doable for a set of applicable entities, regardless of impact category, but longer term implementation schedules are OK where necessary for a given Requirement or set of applicable entities.

Some of the specific questions raised by FERC Technical Staff and the responses provided by the drafting team are as follows:

a) Will Version 5 of the CIP cyber security standards address all of the remaining directives from Order 706? Answer: Yes.

b) Will the drafting team maintain their goals throughout the process?
Answer: Yes

c) Will a document be provided as part of the filing that maps the Order 706 directives to where they are addressed in Version 5? Answer: Yes

d) Did the requirement in CIP-005-4 R1.4 regarding non-critical cyber assets within a defined electronic security perimeter get dropped by mistake in Version 5?
Answer: The drafting team will review and consider the proper place to restore this requirement.

e) FERC Staff asked that a further explanation be provided to define the phrase "system generated list."

Drafting Subteam Questions of FERC Technical Staff

The CSO706 drafting team provided a draft version of its questions of FERC Technical Staff ahead of the meeting **(Appendix 6)**. Many of the questions centered around similar concerns and requirements previously discussed at this meeting. A summary of the discussion that occurred on each question is included below:

Q1: A review of the bright line criteria is needed to ensure that the proper levels of controls are applied to protect the cyber assets. Of particular concern is the bright line between the Medium and Low Impact levels. The drafting team should take another look at the NIST work for more specificity in the controls. Shouldn't all control centers be in the High Impact category considering that they are the "brains" of the system and, if an adversary could gain access to these systems, they could cause the most harm? The drafting team should review the applicable controls and strengthen them where possible. The drafting team might consider a different approach concerning the Low Impact assets (e.g., a secondary table of controls to provide a further breakdown; avoiding a one-size fits all approach for Low Impact assets).

Q2: FERC Staff applauded SDT recognition that non-routable protocols are not immune to attack, and that the SDT is taking appropriate steps to bring these cyber assets under protection. Staff supported the removal of the exception for cyber assets that do not use routable protocols. However, FERC staff was concerned this action this does not adequately address the connectivity issues raised in previous versions, especially as it pertains to applicability. Rather, the controls should protect all Cyber Assets not just those that use routable protocols, and, in cases where there the external connectivity is a non-routable protocol, appropriate controls should be required.

FERC Staff indicated that a technical conference may be planned to address serial connected devices and their associated physical vulnerabilities and cyber vulnerabilities, plus discussion on dial-up and non-routable communications. Hopefully, the results of this conference can be input to Version 5 CIP Standards.

Q3: A better definition of terms, including 'policy', plan, procedure, and program is needed, given that the terms have different meanings across the disciplines responsible for implementing cyber security.

Q4: Unintended and accidental consequences highlight gaps in the requirements that may not be adequately addressed. The drafting team cautions that there may be double jeopardy issues here that need to be addressed as well.

Q5: The drafting team's approach regarding 'immediate revocation' as it is addressed in the standards appears to be on target.

Q6: The FERC Staff indicated that the drafting team's approach regarding deployment of methods to detect malicious attacks needs further review. Clarification is necessary concerning the requirement, since it appears that the requirement is actually stated in the measure. The standard is written to account for a variety of implementations, but the measures specify which solution to employ.

Q7: FERC Staff indicated that further clarification is required with regard to the "two different and complementary" physical access control measures for physical security requirement. The measure seems to state the requirement.

Q8: The issue of 'zero-defects' being required to avoid a violation is a significant concern, but so is 'automatic non-violations'. Need to find a way to encourage a 'find, fix, and don't repeat' culture, but also declare a violation when something 'really bad' happens. More thought is needed here. FERC staff suggested the SDT develop examples and explanations of how/when is this requirement ever violated.

Q9: A more thought-through approach is needed to accomplish the 'maximum capability of a device' requirement. Is the maximum capability the correct solution? How do we encourage industry to move beyond what is in place today, if it is needed to provide the required level of security? Of concern is the possibility that entities may use that requirement to avoid upgrading equipment that could incorporate security enhancements and remain with older more vulnerable equipment.

Next Steps and Action Items

1. The drafting team will take the comments received during today's meeting, assess them, and update the standards to incorporate the thoughts presented.
2. The drafting team will look forward to schedule another possible meeting with the FERC Technical Staff ahead of the posting of the standards for industry comment and ballot. At least another meeting will be scheduled ahead of the filing of the standards for FERC approval.

Adjournment

The Chair thanked everyone for attending this meeting, either in person or via the conference call facilities, and he expressed appreciation on behalf of the drafting team to FERC Technical Staff for their excellent support of this standards drafting development process, and looks forward to FERC staff's continued involvement in the drafting team meetings.

FERC Technical Staff also expressed their appreciation to the drafting team for organizing this meeting and for the open and frank discussions. The FERC Technical Staff was encouraged by the conduct of the meeting and of the standards development process, and invited the drafting team to schedule another meeting in the near future.

The meeting adjourned at approximately 4:30 p.m. on Thursday, July 28, 2011.

Appendix 1 - Agenda

Thursday, July 28, 2011 from 9:00 am – 5:00 pm Eastern Time

Conference Number: 1-866-740-1260

Conference Code: 9815445

Administrative Items

9:00 am Introductions — All

9:15 am NERC Antitrust Compliance Guidelines – Joe Bucciero

9:20 am Agenda and Objectives — John Lim/Phil Huff

Brief Status of CIP Version 5 Standards Development

9:30 am Overview Presentation of CIP Standards and Concepts – John Lim

10:00 am Review Project Schedule Highlights – Phil Huff/Joe Bucciero

10:15 am *Stretch Your Legs Break (5 minutes)*

FERC Staff Questions for Standard Drafting Team

10:20 am FERC Staff Questions – Part 1

11:30 am *Lunch*

12:30 pm FERC Staff Questions – Part 2

2:30 pm *Afternoon Break*

Standard Drafting Team Questions to FERC Staff

2:45 pm Standard Drafting Team Questions – Part 1

3:45 pm *Stretch Your Legs Break (5 minutes)*

3:50 pm Standard Drafting Team Questions – Part 2

Next Steps – John Lim/Phil Huff/Joe Bucciero

4:15 pm Discussion of Outstanding Tasks

Action Items – Joe Bucciero

4:30 pm Review Action Items

Adjourn

Appendix 2
Members Attending
In Person or via ReadyTalk and Phone

Name	Company
1. Rob Antonishen	Ontario Power Generation
2. Jay Cribb	Southern Company Services
3. Gerry Freese	AEP
4. Philip Huff, Vice Chair	Arkansas Electric Coop Corporation
5. Doug Johnson	Exelon Corporation – Commonwealth Edison
6. John Lim, Chair	**Consolidated Edison Co. NY**
7. David Revill	Georgia Transmission Corporation
8. Tom Stevenson	Constellation
9. John Varnell	Tenaska
10. William Winters	Arizona Public Service.
Joe Bucciero	*NERC Facilitator*
Holly Hawkins	*NERC Staff*
Scott Mix	*NERC Staff*
Steve Noess	*NERC Staff*
Andy Rodriquez	*NERC Staff*

Others Attending In Person or via ReadyTalk and Phone

Matthew Adeleke, Megan Aikman, Joseph Andrews, Jan Bargen, James Batug, David Batz, Bruce Bingham, Jim Brenton, Thomas Brownback, Jackie Collett, Matt Dale, David Dockery, Ted Franks, John Fridye, Lori Hayes, David Huff, Chris Jager, Annette Johnston, Michael Keane, Morgan King, Kim Koster, Barry Kuehnle, Barry Lawson, Vincent Le, Andres Lopez, Sharon Mayers, Patrick Miller, Nathan Mitchell, Craig Nelson, Brian Newell, Wilket Ng, Dave Norton, Claudine Planter-Pascal, Mike Peters, James Phillips, Austin Rappeport, David Rivera, Kevin Ryan, Katie Schnider, Bryn Wilson, Jian Zhang

APPENDIX 3 - CYBER SECURITY ORDER 706 STANDARD DRAFTING TEAM (PROJECT 2008-06)

1. Chairman	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
2. Vice Chairman	Philip Huff Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
3. Members	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@opg.com
4.	René Bourassa	Hydro Québec 6100 Des Forges Trois-Rivières, QC G8Y6K5	(819) 694-2507 bourassa.rene@hydro.qc.ca
5.	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
6.	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@ duke-energy.com
7.	Gerald S. Freese Director, NERC CIP Compliance	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
8.	Christine Hasha Compliance Analyst Senior	Electric Reliability Council of Texas 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3909 (512) 248-3993 Fx christine.hasha@ ercot.com
9.	Jeffrey Hoffman Chief Architect, IT Policy and Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm 380 P.O. Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 jhoffman@usbr.gov
10.	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon – Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com

11.	Robert Preston Lloyd Sr. Technical Specialist, Substation Regulatory Compliance	SC&M Technical Support & Strategy Southern California Edison One Innovation Way Pomona, CA 91768	(626) 543-7863 (909) 274-1338 (626) 422-1346 M robert.lloyd@sce.com
12.	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
13.	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@gatrans.com
14.	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	Tom Hofstetter Regional Compliance Auditor	North American Electric Reliability Corporation 3353 Peachtree Rd NE North Tower, Suite 600 Atlanta, GA 30326	(609) 452-8060 (609) 452-9550 fax tom.hofstetter@ nerc.net
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 3353 Peachtree Rd NE North Tower, Suite 600 Atlanta, GA 30326	(609) 452-8060 (609) 452-9550 fax roger.lampila@ nerc.net
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 3353 Peachtree Rd NE North Tower, Suite 600 Atlanta, GA 30326	(215) 853-8204 (609) 452-9550 fax scott.mix@ nerc.net
NERC Staff	Steven Noess Standards Development Advisor	North American Electric Reliability Corporation 3353 Peachtree Rd NE North Tower, Suite 600 Atlanta, GA 30326	(404) 446-9691 (404) 217-7578 M steven.noess@ nerc.net
NERC Staff	Andy Rodriquez Director of Standards Development	North American Electric Reliability Corporation 3353 Peachtree Rd NE North Tower, Suite 600 Atlanta, GA 30326	(609) 947-3885 andy.rodriquez@ nerc.net

Appendix 4 – Project and Meeting Schedule

Meeting Location	Dates	Meeting Objective
Salt Lake City, UT WECC	**7/19 to 7/21/2011**	**Walk-through sample generation and substation environments with the Version 5 requirements to determine feasibility. Output additional guidance based on the walk-through process**
Interim	7/22 to 8/15/2011	Revise drafting requirements based on feedback from walk-through process – **primarily agree to the use of defined terms External Connectivity, BES Cyber System and Routable External Connectivity** Drafting leads prepare for August Meeting with representatives from Industry stakeholder organizations
Washington, DC	7/28/2011	Drafting Team Meeting with FERC Staff
Atlanta, GA NERC	**8/16 to 8/18/2011**	**Review of Standards with Industry Representatives**
Interim Week 1	8/19 to 8/26/2011	Revise drafting requirements based on feedback from Industry Representatives
WEBINAR	***8/24/2011***	***Industry Webinar as outreach to present concepts and schedule for Version 5 CIP Standards***
Interim Week 2	8/25 to 9/2/2011	Revise drafting requirements based on feedback from Industry Representatives
LABOR DAY	*9/5/2011*	*Labor Day Holiday*
Interim Week 3	9/6 to 9/9/2011	Update rationale, change documentation and guidance to reflect requirements
Interim Week 4	9/12 to 9/16/2011	Review VRFs and VSLs modified from Version 4 Review CIP-010 and 011 informal comment/response document

Meeting Location	Dates	Meeting Objective
Westminster, CA SCE	**9/20 to 9/22/2011**	**CSO706 Drafting Team approves CIP Standards, implementation plan, and other documentation for NERC Quality Review (QR)**
Quality Review Prep	9/23/2011	Finalize and Issue Version 5 Documents for NERC Quality Review
NERC Quality Review	9/26 to 10/14/2011	NERC Quality Review & meeting with DT leadership and subteam leads to provide comments
Interim	10/17 to 10/24/2011	Subteams to review and update standards and all documentation based on QR and prepare for posting
Constellation Baltimore, MD	**10/25 to 10/27/2011**	**SDT Meeting to consider QR changes made to the standards and finalize standards for posting**
Interim	10/28 to 11/2/2011	SDT Finalizes CIP V5 Documents for Posting
POSTING	*11/3/2011*	*Post CIP Standards for 45+ day formal comment with concurrent ballot*
Comment & Ballot Period	11/4 to 12/19/2011	Version 5 CIP Standards 45+ day formal Comment and Ballot Period
	11/4 to 11/14/2011	SDT Members Prepare for Industry Webinar on CIP V5 Standards
WEBINAR	***11/15/2011***	***Industry Webinar as outreach to present concepts and schedule for Version 5 CIP-002 standard requirements, the overall format of the standards, the definitions used and the implementation plan.***
	11/16 to 11/28/2011	SDT Members Prepare for Industry Webinar on CIP V5 Standards
WEBINAR	***11/29/2011***	***Industry Webinar as outreach to present concepts and schedule for Version 5 CIP-003 through CIP-011 Standards***

Meeting Location	Dates	Meeting Objective
Web Conference	**11/30 to 12/1/2011**	**Drafting Team Meeting to review Webinar questions and comments**
	12/20 to 12/21/ 2011	NERC Staff Prepares Industry Comments and Ballot Comments Received for Review by SDT
Review Comments	12/22/2011 to 1/23/2012	Review formal comments and concurrent ballot comments. NERC will prepare initial draft responses to comments for SDT consideration. SDT to begin update of standards text based on feedback received through industry comments and ballot comments.
FRCC (Tampa, FL)	**1/24 to 1/26/2012**	**Drafting Team Meeting to review initial responses to comments, prepare additional responses to formal comments and ballot comments, and continue to update text of standards**
Interim	1/27 to 2/10/2012	Drafting Team prepares updates to the CIP standards text based on feedback from 45-day comment and ballot period
Interim	2/13 to 2/20/2012	Continue to review industry comments and incorporate changes into the text of the standards Revise standards for re-posting for 30-day comment and ballot period
APS (Phoenix, AZ)	**2/21 to 2/23/2012**	**Drafting Team Meeting to finalize & approve responses to formal comments and finalize standards documents for Quality Review.** **SDT to prepare documents for NERC QR**
NERC Quality Review	2/24 to 3/9/2012	NERC Quality Review of Responses to Industry Comments from 45-day comment & ballot period. Quality Review of related updates to the CIP standards
Interim	3/12 to 3/19/2012	SDT updates standards and all documentation based on QR and prepares for posting for 30-day comment & ballot period

Meeting Location	Dates	Meeting Objective
WEB Conference	**3/20 to 3/21/2012**	**SDT Meeting to consider QR changes made to the standards and finalize standards for 30-day formal comments and successive ballot posting**
Interim	3/22 to 3/23/2012	NERC Prepares Documents for Successive Ballot
POST Responses to Comments	*3/26/2012*	*Post responses to 45-day formal comments with concurrent ballot comments*
Comment & Ballot	*3/26 to 4/27/2012*	*30-day Posting of CIP Standards for comments with successive ballot*
Interim	3/26 to 4/25/2012	Begin preparation of FERC filing documentation
Interim	4/30 to 5/1/2012	NERC Staff Prepares Industry Comments and Ballot Comments Received for Review by SDT
Interim	5/2 to 5/22/2012	Subteam meetings to prepare responses to successive ballot comments and revise text of CIP Standards, as necessary
Location (??)	**5/22 to 5/24/2012**	**Drafting Team Meeting to finalize responses to comments and prepare revisions to CIP Standards for recirculation ballot (10-days)**
NERC Quality Review	5/25 to 6/8/2012	NERC Quality Review of Responses to Industry Comments from 30-day comment & ballot period Quality Review of related updates to the CIP standards
Post for Ballot	*6/11/2012*	*Post for recirculation ballot*
Interim	6/11/2012 6/22/2012	Recirculation Ballot
Finalize Standards	*6/25 to 6/29/2012*	*Finalize CIP standards text for approval by NERC BOT*

NEED, GOALS AND OBJECTIVES – PROJECT 2008-06 - CIP CYBER SECURITY STANDARDS V5 – ADOPTED JANUARY 2011

NEED

The need for Critical Infrastructure Protection (CIP) in North America has never been more compelling or necessary than it is today. This is especially true of the electricity sector. Electric power is foundational to our social and economic fabric, acknowledged as one of the most essential and among the most targeted of all the interrelated critical infrastructure sectors.

The Bulk Electric System (BES) is a complex, interconnected collection of facilities that increasingly uses standard cyber technology to perform multiple functions essential to grid reliability. These BES Cyber Systems provide operational efficiency, intercommunications and control capability. They also represent an increased risk to reliability if not equipped with proper security controls to decrease vulnerabilities and minimize the impact of malicious cyber activity.

Cyber attacks on critical infrastructure are becoming more frequent and more sophisticated. Stuxnet is a prime example of an exploit with the potential to seriously degrade and disrupt the BES with highly malicious code introduced via a common USB interface. Other types of attacks are network or Internet-based, requiring no physical presence and potentially affecting multiple facilities simultaneously. It is clear that attack vectors are plentiful, but many exploits are preventable. The common factors in these exploits are vulnerabilities in BES Cyber Systems. The common remedy is to mitigate those vulnerabilities through application of readily available cyber security measures, which include prevention, detection, response and recovery.

In the cyber world, security is truly only as good as its weakest implementation. The need to identify BES Cyber Systems and then protect them through effective cyber security measures are critical steps in helping ensure the reliability of the BES functions they perform.

In approving Version 1 of CIP Standards CIP-002-1 through CIP-009-1, FERC issued a number of directives to the ERO. Versions 2, 3 and 4 addressed the short term standards-related and Critical Asset identification issues from these directives. There are still a number of unresolved standards-related issues in the FERC directives that must be addressed. This version is needed to address these remaining directives in FERC Order 706.

GOALS AND OBJECTIVES

- **Goal 1:** To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.
    - **Objective 1.** Provide a list of each directive with a description and rationale of how each has been addressed.
    - **Objective 2.** Provide a list of approved interpretations to existing requirements with a description of how each has been addressed.
    - **Objective 3.** Provide a list of CAN topics with a description of how each has been addressed.
    - **Objective 4.** Consider established security practices (e.g. DHS, NIST) when developing requirements.
    - **Objective 5.** Incorporate the work of Project 2010-15 Urgent Action SAR.
- **Goal 2:** To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.
    - **Objective 6**: Transition from a Critical Cyber Asset framework to a BES Cyber System framework.
    - **Objective 7.** Develop criteria to identify and categorize BES Cyber Systems, leveraging industry approved bright-line criteria in CIP-002-4.
    - **Objective 8.** Develop appropriate cyber security requirements based on categorization of BES Cyber Systems.
    - **Objective 9.** Minimize writing requirements at the device specific level, where appropriate.

- **Goal 3:** To provide guidance and context for each Standard Requirement
  - **Objective 10.** Use the Results-Based Standards format to provide rationale statements and guidance for all of the Requirements.
  - **Objective 11.** Develop measures that describe specific examples that may be used to provide acceptable evidence to meet each requirement. These examples are not all inclusive ways to provide evidence of compliance, but provide assurance that they can be used by entities to show compliance.
  - **Objective 12.** Work with NERC and regional compliance and enforcement personnel to review and refine measures.
- **Goal 4:** To leverage current stakeholder investments used for complying with existing CIP requirements.
  - **Objective 13.** Map each new requirement to the requirement(s) in the prior version from which the new requirement was derived.
  - **Objective 14.** Justify change in each requirement which differs from the prior version.
  - **Objective 15.** Minimize changes to requirements which do not address a directive, interpretation, broad industry feedback or do not significantly improve the Standards.
  - **Objective 16.** Justify any other changes (e.g. removals, format)
- **Goal 5:** To minimize technical feasibility exceptions.
  - **Objective 17.** Develop requirements at a level that does not assume the use of specific technologies.
  - **Objective 18.** Allow for technical requirements to be applied more appropriately to specific operating environments (i.e. Control Centers, Generation Facilities, and Transmission Facilities). (also maps to Goal 2)
  - **Objective 19.** Allow for technical requirements to be applied more appropriately based on connectivity characteristics. (also maps to Goal 2)
  - **Objective 20.** Ensure that the words "where technically feasible" exist in appropriate requirements.
- **Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to compliment a "culture of compliance".
  - **Objective 21.** Work with NERC Compliance Staff to evaluate options to reduce compliance impacts such as continuous improvement processes, performance based compliance processes, or SOX-like evaluation methods.
  - **Objective 22.** Write each requirement with the end result in mind, (minimizing the use of inclusive phrases such as "every device," "all devices," etc.)
  - **Objective 23.** Minimize compliance impacts due to zero-defect requirements.

- **Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
  - **Objective 24.** Avoid per device, per requirement compliance dates**.**
  - **Objective 25.** Address complexities of having multiple versions of the CIP standards in rapid succession.
  - **Objective 26.** Consider implementation issues by setting realistic timeframes for compliance.
  - **Objective 27.** Rename and modify IPFNICCAANRE to address BES Cyber System framework.

Appendix 6 - Questions for FERC Technical Staff on NERC CIP V5 Working Draft

1. In its development of CIP-002-5, the SDT used a 3 tier categorization for the application of controls based on impact of BES Cyber Systems to the BES: large control centers (e.g., RC, BA, TOP) for High Impact, significant impact field transmission and generation assets and other control centers for Medium Impact, and remaining field assets for Low Impact. This approach is based on criteria developed in Version 4, currently filed for consideration by FERC. The SDT seeks FERC technical staff's comment on the approach to categorization of BES Cyber Systems and BES Cyber Assets.

2. The SDT removed the exception for cyber assets that do not use routable protocols that was included in previous versions of CIP-002. The SDT has addressed differences due to connectivity type as an applicability issue, where warranted, on a per requirement basis. The SDT seeks FERC technical staff's opinion on whether this adequately addresses the connectivity issue raised in previous versions.

3. In CIP-003-5, the SDT has removed requirements relating to exceptions to entities' security policies since it considers this a general management issue that is not within the scope of a compliance requirement. This is considered to be an internal policy requirement and not a reliability requirement. The SDT seeks FERC staff's comment on this approach.

4. The FERC Order directed the drafting team to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The drafting team has attempted to address this directive by requiring a framework for the configuration management process that includes a documented baseline configuration, explicit authorization for changes, and configuration monitoring for High Impact BES Cyber Systems. The SDT seeks FERC technical staff's comment on this approach.

5. In CIP-004-5, in the revocation of access section, the SDT has specified ***immediate revocation of the ability to access*** cyber systems for terminated personnel or personnel no longer requiring access to cyber systems. The SDT seeks FERC's comments on this issue.

6. In CIP-005-5, the SDT has included a requirement for detecting intrusions or malicious communication (IDS) in addition to access control and monitoring of the electronic access points in response to FERC's comments on defense in depth. The SDT seeks FERC technical staff's comment on the SDT's approach.

7. In CIP-006-5, the SDT has included a requirement for at least two "different and complementary" physical access control measures for the physical security boundary in response to FERC's comments on defense in depth. The SDT seeks FERC technical staff's comment on the SDT's approach.

8. The SDT has included process improvement features in CIP-004-5 R6 and CIP-007-5 R4 that addresses the problem of zero defect in current corresponding requirements. The SDT requests FERC technical staff's comments on this approach.

9. The SDT has used "to the maximum capability of a device" in seven requirements. The SDT has used this approach to avoid drafting to the lowest common denominator, while providing the most appropriate level of the cyber security control in the requirement. The use of this phrase requires the entity to use the maximum capability of the BES Cyber Asset or BES Cyber System to meet the requirement in instances where device limitations otherwise preclude meeting the thresholds. The SDT believes that this provides, where appropriate, the necessary oversight through the requirements language for legacy devices and the existing audit process, without the need for the additional overhead of a Technical Feasibility Exception. The SDT requests FERC technical staff's comments on this approach.

Appendix 7 – CIP Standards Development Overview (Hyperlink)