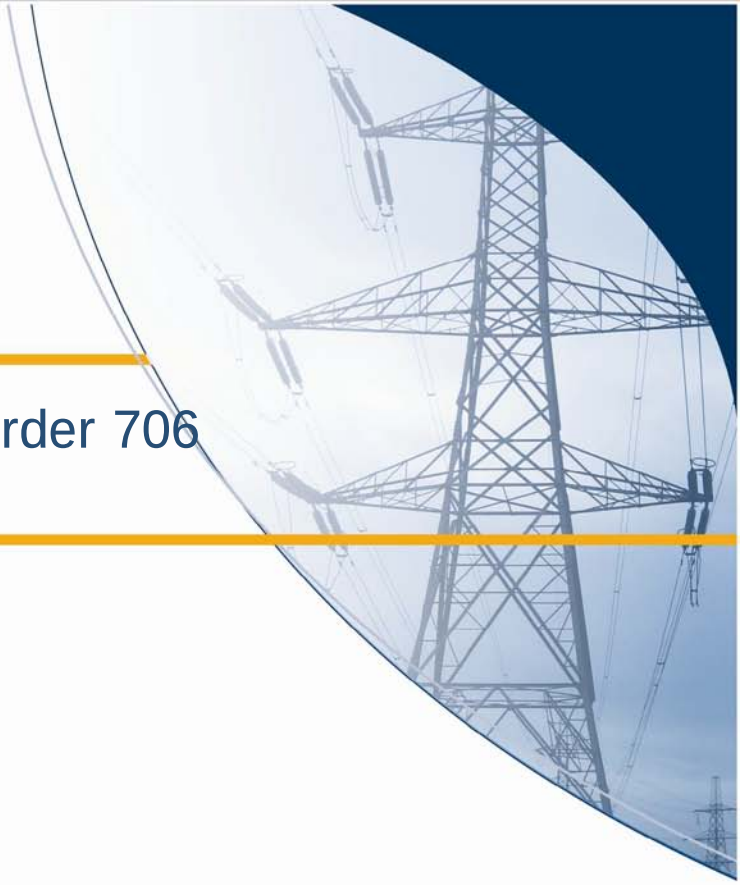
NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Project 2008-06 Cyber Security Order 706
31st Meeting Summary

Taylor, TX

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

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

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT- Project 2008-06
31ST MEETING
February 15-17, 2011
Taylor, Texas

Executive Summary

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Taylor and thanked Jim Brenton at ERCOT for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Tuesday morning, the SDT unanimously adopted the January 18-20, 2011 Columbus meeting summary. The chair outlined the objectives the SDT sought to accomplish by the end of the meeting that included team agreement on whether to post CIP Version 5 as a single standard or multiple standards, evaluation of options with NERC Compliance staff to minimize excessive compliance costs while improving overall cyber security, reviewing and refining CIP Version 5 BES Cyber System identification and security requirements, and agreement on team next steps and assignments.

The Chair reported to that team that Jon Stanford, formerly of Bonneville Power Association, had submitted his resignation from the SDT. The team expressed its appreciation for his participation. Also, Jim Brenton announced a change of role at ERCOT and asked to be replaced by a colleague. Due to the number of resignations over the past two meetings, the team is asking the Standards Committee at its March meeting to appoint Robert Preston Lloyd to replace Patricio Leon-Alvarado and Christine Hasha to replace Jim Brenton. The team still desires another Canadian representative, which is posted as a vacancy for the team.

Scott Mix provided an update on the recent progress on the project for updates to CIP-005-4 regarding remote access. The team for Project 2010-15 is continuing to develop responses to comments and modify the proposed requirement in response to comments. That team is still working toward the goal of submitting the approved revised CIP-005-4 to FERC in time for the commission to act in conjunction with the CIP-002-4 action.

The team reviewed the Needs, Goals, and Objectives document that was developed and adopted at the Columbus meeting, and is provided in **Appendix 3**. The current makeup of each sub-team is provided in **Appendix 4**.

The team then considered the issue of the format of the next version of the CIP standards. The document in **Appendix 5** was presented to start discussion. After discussion, the chair then asked each person to provide feedback on their position and what they were hearing from industry. A summary of the feedback given by each person is provided in **Appendix 6**. Based on this discussion the following proposal was developed:

> Maintain the CIP-002 through CIP-009 structure and build on the sub-team work performed by the SDT on the new requirements. Then create a small group to craft a CIP-002 to CIP-00x for comparison between old and new formats.

The team adopted this proposal with 13 affirmative, 1 negative, and 1 abstention. The chair will assemble a small group to divide CIP-011 into a CIP-003 to CIP-00x proposal.

The team then held a discussion with Valerie Agnew with NERC Compliance staff. Based on the results of that discussion, the team decided it needed to reexamine the requirements at the Low level to determine whether the benefit derived was worth the effort expended to be compliant.

On February 16, the team began the meeting with a discussion on methods to reach out to existing industry group to aid in development and education on the next set of CIP standards. The team decided on the following action items:

- Send the team schedule and draft products to the new DOE, NIST, and NERC cyber security initiative.
- Each SDT member is to send a list of groups they are active in to Howard Gugel to assist the SDT in its outreach.
- Ensure there are talking points developed prior to the outreach.

The BES Cyber System Categorization sub-team presented its latest version of CIP-010 to the group. There was considerable conversation around the exclusion language for 4.2.2. After failing to achieve a resolution of the issue, the sub-team agreed to revisit the issue and propose a solution at the next meeting.

The Change Management, System Lifecycle, Information Protection, Maintenance, Governance, and Vulnerability Assessments sub-team then reported on their assigned requirements in CIP-011. There was considerable conversation about the issue of Media Sanitization. The following proposal was agreed to by consent:

- Media sanitization will be moved to CIP-007. Then the definition of media is no longer needed.

The issue of what should be included in a Responsible Entity's security policy. The following proposal was agreed to by consent:

- Management's commitment to the cyber protection of its BES Cyber Systems

The Personnel and Physical Security sub-team then reported on their assigned requirements in CIP-011. There was considerable discussion around the issues of personnel training and personal risk assessment. The sub-team team agreed to take the conversation into account and return to the next meeting with a proposed alternative or justification for the current draft.

On February 17, the team began the meeting with a discussion on schedule. Howard Gugel presented that the Standards Committee had approved a revised schedule for the team that would require posting the next version of the CIP standards for formal comment and ballot by the end of 2011. The team would be expected to deliver the approved set of standards to the Board of Trustees by the end of the second quarter of 2012. The team agreed and the revised schedule is shown in **Appendix 7**.

The team then held a discussion about the level to which the requirements should be written. Some felt that all requirements should be at a high level. Some felt that industry was looking to the team to tell them exactly what was needed to be compliant. Finally, the team agreed to use the following questions when evaluating all drafted requirements:

1. Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? This may be the real requirement
2. Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? May be too specific.
3. Is the timeframe arbitrary?
4. Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

The Access Control sub-team then reported on their assigned requirements in CIP-011. The sub-team reported that they had difficulty writing the requirements at a high level. Next, the System Security and Boundary Protection sub-team reported on their assigned requirements in CIP-011.

Finally, the team discussed revising the style guide to incorporate suggested improvements. The revised style guide is provided as **Appendix 8**.

The meeting attendees were asked to complete a meeting evaluation. A summary of the results of the responses is provided in **Appendix 9**. These results will be used in planning future meetings of the SDT.

The Chair thanked Jim Brenton, Christine Hasha and ERCOT for the hosting of the SDT in Taylor.

The meeting adjourned at 5:00 on Thursday, February 17, 2011

Appendix 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
31st Meeting Agenda
February 15, 2011 Tuesday - 8:00 AM to 6:00 PM CST
February 16, 2011 Wednesday - 8:00 AM to 6:00 PM CST
February 17, 2011 Thursday - 8:00 AM to 6:00 PM CST
ERCOT
800 Airport Drive, Taylor, TX

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

Meeting Objectives/Outcomes:

- To agree on whether to post CIP Version 5 as a single standard or multiple standards
- To evaluate options with NERC compliance staff to minimize excessive compliance costs while improving cyber security
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Tuesday, January 18, 2011 8:00 a.m. - 6:00 p.m. CST

- Introduction, welcome -*(Morning)*
- NERC staff support update *(Morning)*
- Industry review: (*Morning*)
    - DOE Audit Report
    - FERC Technical Conference
    - Cyber Attack TF and Severe Impact Resilience TF
    - CIP-005-4 Update
- Review and agree on CIP format for posting *(Morning)*
- Evaluate "culture of security" options with NERC compliance *(Afternoon)*
    - Writing programmatic requirements
    - Minimizing zero-defect requirements
    - Minimizing and improving TFE process

Wednesday, January 19, 2011 8:00 a.m. - 6:00 p.m. CST

- Review and refine BES Cyber System Identification (*Morning/Early Afternoon*)
- Review modifications to style guide (*Afternoon)*
- Review and refine security requirements (*Afternoon*)

Thursday, January 20, 2011 8:00 a.m. - 6:00 p.m. CST

- Review and refine security requirements (*Morning/Afternoon*)
- Review and agree to next steps and drafting assignments (*Late Afternoon*)
- Review communication plan for CIP V5 (*Late Afternoon*)
- Review SDT March, 2011 New York, NY Meeting (*Late Afternoon)*

Appendix 2—Attendees List
February 15-17, 2011 Taylor

Attending in Person — SDT Members and Staff

1. Jim Brenton	ERCOT
2. Jay Cribb	Southern Company Services
3. Joe Doetzl	Kansas City Pwr. & Light Co
4.Jerry Freese	America Electric Pwr.
5. Philip Huff, Vice Chair	Arkansas Electric Coop Corporation
6. Doug Johnson	Exelon Corporation – Commonwealth Edison
7.Rich Kinas	Orlando Utilities Commission
8. John Lim, Chair	Consolidated Edison Co. NY
9. David Revill	Georgia Transmission Corporation
10. Scott Rosenberger	Luminant Energy
11. Kevin Sherlin	Sacramento Municipal Utility District
12. Tom Stevenson	Constellation
13. Keith Stouffer	National Institute of Standards & Technology
14. William Winters	Arizona Public Service, Inc.

SDT Members Attending via ReadyTalk and Phone

15. Rob Antonishen	Ontario Power Generation
16.Sharon Edwards	Duke Energy
17. John D. Varnell	Tenaska Power Services Co.
18. John Van Boxtel	Portland General
Scott Mix	*NERC*
Howard Gugel	*NERC*
Roger Lampila	*NERC*
Valerie Agnew	*NERC*

SDT Members Not Participating

Bill Gross	NEI
Jeff Hoffman	USBR

Others Attending in Person

Robert Preston Lloyd	Southern California Edison
Jim Fletcher	American Electric Power
Jason Marshall	Midwest ISO
John Carpenter	ERCOT
Brian Newell	American Electric Power
David Dockery	AECI
Mike Keane	FERC
Christine Hasha	ERCOT
Ryan Breed	ERCOT
Matt Stout	ERCOT
Scott Raymond	ERCOT
Ken McIntyre	ERCOT
Alan Rivaldo	PUCT
David Grubbs	City of Garland, TX

Others Attending via Readytalk and Phone

February 15
Patricio Leon, Roger Fradenburgh, Jan Bargen, Dave Norton, Katie Schnider, Dave Burtrum, Paul Franson, David Dunn, David Gordon

February 16
Dave Burtrum, Patricio Leon, John Fridye, David Gordon, Jan Bargen

February 17
Dave Burtrum, David Gordon, Jan Bargen, Bryn Wilson, John Fridye, Patricio Leon

Appendix 3

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

NEED

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

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

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

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

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

GOALS AND OBJECTIVES

- **Goal 1:** To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.
  - **Objective 1.** Provide a list of each directive with a description and rationale of how each has been addressed.
  - **Objective 2.** Provide a list of approved interpretations to existing requirements with a description of how each has been addressed.
  - **Objective 3.** Provide a list of CAN topics with a description of how each has been addressed.
  - **Objective 4.** Consider established security practices (e.g. DHS, NIST) when developing requirements.
  - **Objective 5.** Incorporate the work of Project 2010-15 Urgent Action SAR.
- **Goal 2:** To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.
  - **Objective 6**: Transition from a Critical Cyber Asset framework to a BES Cyber System framework.
  - **Objective 7.** Develop criteria to identify and categorize BES Cyber Systems, leveraging industry approved bright-line criteria in CIP-002-4.
  - **Objective 8.** Develop appropriate cyber security requirements based on categorization of BES Cyber Systems.
  - **Objective 9.** Minimize writing requirements at the device specific level, where appropriate.
- **Goal 3:** To provide guidance and context for each Standard Requirement
  - **Objective 10.** Use the Results-Based Standards format to provide rationale statements and guidance for all of the Requirements.
  - **Objective 11.** Develop measures that describe specific examples that may be used to provide acceptable evidence to meet each requirement. These examples are not all inclusive ways to provide evidence of compliance, but provide assurance that they can be used by entities to show compliance.
  - **Objective 12.** Work with NERC and regional compliance and enforcement personnel to review and refine measures.
- **Goal 4:** To leverage current stakeholder investments used for complying with existing CIP requirements.

- **Objective 13.** Map each new requirement to the requirement(s) in the prior version from which the new requirement was derived.
- **Objective 14.** Justify change in each requirement which differs from the prior version.
- **Objective 15.** Minimize changes to requirements which do not address a directive, interpretation, broad industry feedback or do not significantly improve the Standards.
- **Objective 16.** Justify any other changes (e.g. removals, format)

- **Goal 5:** To minimize technical feasibility exceptions.
  - **Objective 17.** Develop requirements at a level that does not assume the use of specific technologies.
  - **Objective 18.** Allow for technical requirements to be applied more appropriately to specific operating environments (i.e. Control Centers, Generation Facilities, and Transmission Facilities). (also maps to Goal 2)
  - **Objective 19.** Allow for technical requirements to be applied more appropriately based on connectivity characteristics. (also maps to Goal 2)
  - **Objective 20.** Ensure that the words "where technically feasible" exist in appropriate requirements.
- **Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to complement a "culture of compliance".
  - **Objective 21.** Work with NERC Compliance Staff to evaluate options to reduce compliance impacts such as continuous improvement processes, performance based compliance processes, or SOX-like evaluation methods.
  - **Objective 22.** Write each requirement with the end result in mind, (minimizing the use of inclusive phrases such as "every device," "all devices," etc.)
  - **Objective 23.** Minimize compliance impacts due to zero-defect requirements.
- **Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
  - **Objective 24.** Avoid per device, per requirement compliance dates**.**
  - **Objective 25.** Address complexities of having multiple versions of the CIP standards in rapid succession.
  - **Objective 26.** Consider implementation issues by setting realistic timeframes for compliance.
  - **Objective 27.** Rename and modify IPFNICCAANRE to address BES Cyber System framework.

Appendix 4—SDT Sub-Teams

Sub-Team	
BES Cyber System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton *(Christine Hasha ?)* *(Observer Participants: Rod Hardiman, Jim Fletcher, Robert Preston Lloyd, David Burtrum, Bryn Wilson)* *(FERC: Mike Keane,)*
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, David Burtrum)* *(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, Robert Preston Lloyd)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, Governance, and Vulnerability Assessments	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*

Appendix 5

CIP-002 to CIP-009 Format

PRO	CON
The current de-facto standard format that the industry is familiar with	Terms used across more than one standard must go in the NERC glossary and be used across all NERC standards.
May require less change in entities' existing compliance documentation at the standard level	Today there is much cross referencing between requirements across standards which could be simplified if all the requirements were in one standard. Examples include CIP-005 R1.5 and CIP-006 R2.2. Access control is spread throughout several standards.
Appears to have much broader support across industry, including trade organizations	The individual standards are not stand-alone as each NERC standard should be. Changes to one result in changes to all others to keep all in sync. Resolving the issue above will mitigate this issue.
Less investment in existing tools required to maintain compliance documentation	With the amount of anticipated modifications, change to documentation (and amount of documentation) may be higher than if combined in CIP-011.
Addition/deletion of requirements only affects renumbering a small number of requirements, as opposed to many if all requirements are in one standard.	If local definitions are repeated across multiple standards, changes to those definitions would need to be tracked across those standards. (con for CIP-003 to 9)

CIP-010 and CIP-011 Format

PRO	CON
Gathering all cyber security requirements into one standard makes that one standard, once converted to, more future-proof.	Requires a reorganization of compliance materials on the part of all entities.
Allows for local definitions within the single standard that can apply across all cyber security areas. No effects of defining terms for cyber use on other standards.	Future revision issues with items numbers and grouping of topics
Possible different grouping of requirements ties **To other industry standard organization models (NIST, ISO, ETC).**	May inflate the violation statistics when reported at the Standard level and all cyber violations are against one standard.
Helps highlight the paradigm shift from Critical Cyber Assets to BES Cyber Systems.	It will be difficult to track repeat violations across version 4 to version 5.

NOTE: Repeat violations are determined at the requirement level, not the standard level. Violations are often reported in aggregate at the standard level. A change to a combined format where all cyber security requirements are in one standard should have no effect on the repeat violation determination.

Appendix 6

Feedback on CIP Version 5 by participant

Joe Doetzl	Format is not an issue, requirements are. There are no strong proponents of CIP-010 and CIP-011 outside of the room. Preference for CIP-002 to CIP-009
Doug Johnson	CIP-002 to CIP-009 is preferable. Most thought CIP-010 and CIP-011 were dead.
Jim Fletcher	There are substantial changes. Use this opportunity to gather consensus. Provide rationale for decisions. Put results out to industry, and help them come to the same decision.
Scott Rosenberger	UNITE is for CIP-002 to CIP-009. If we proceed with CIP-010 and CIP-011, industry will say "You didn't listen."
Jay Cribb	"Evolution is preferable to revolution." Those that get CIP-010 and CIP-011, get it. Even if we keep CIP-002 to CIP-009, words will need to stay the same. The requirements will drive the decision.
Bill Winters	Better have a real good reason to change from CIP-002 to CIP-009. Need marketing campaign to get it to pass. There are a lot of organizations that are not currently implementing CIP-003 to CIP-009 based on CIP-002. What are their opinions?
Robert Lloyd	We've discussed this many times. Anything we do will be a change.
Keith Stouffer	People that look at CIOP-010 and CIP-011 like it for security, BUT compliance issue is huge. People have existing programs. Overwhelmingly heard CIP-003 to CIP-009. Shelving new paradigm may cause issue.
John Lim	Not a lot of support for CIP-010 and CIP-011 in its current format. We ned to make allowances. Seems to be overwhelming support for CIP-002 to CIP-009
Kevin Sherlin	Content significantly more important than format.
Rich Kinas	Many aggressively support maintaining CIP-003 to CIP-009. Some support the concept of CIP-010 and CIP-011, but do not actively support it.
Jim Brenton	It has been a journey. There were issues in CIP-003 to CIP-009 for transmission and generation. Jim is interested in content, not form. The need cannot be met with a "tweek." Compliance program should not drive standard development.
Christine Hasha	Much input on renumbering. CIP-010 and CIP-011 is good to show shift in direction. Eliminate "spaghetti" requirements.
David Revill	This is a change management issue. Concentrate on content, not format.
Mike Keane	(Speaking for himself, not the Commission) Get the requirements right. Get response to Order 706 correct. Write a minimum set of standards for all BES Cyber Assets.

Scott Mix	CIP-010 and CIP-011 provides a paradigm shift and change. Also provides flexibility to target environments.
Philip Huff	His organization does not care. CIP-010 and CIP-011 can be divided along a CIP-003 to CIP-009 structure.
Tom Stevenson	Those that like CIP-003 to CIP-009 currently want to keep them. Those that are new to the process prefer CIP-010 and CIP-011, but opinions differ by operating environment.
Jerry Freese	We must explain very thoroughly our rationale. We are supposed to be doing security, not compliance. No gaps on either side. We just need to package it correctly.
Sharon Edwards	Many that support CIP-002 to CIP-009 erroneously believe that this will limit controls to all BES Cyber Assets. Doing CIP-003 to CIP-009 may minimize impact to the industry.

Appendix 7

CSO706 SDT
Meeting Schedule and Objectives (February 2011)

Development Process

- Face-to-face meetings used to review/refine the entire Standard. Full team reviews Standards to raise issues, formulate concepts to address issues, ensure consistency across sub-teams and further develop work products.
- Sub-teams meet in open web conferences in between face-to-face meetings to address issues raised by the full team.
- Full team 2 hour web conference the 2nd Thursday from 12:00a – 2:00p after every full team meeting to receive sub-team status updates and provide initial feedback.

Meeting Location	Dates	Meeting Objective
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	Full review of Standards Initial discussions on implementation plan. 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 of Standards and implementation plan
Interim	4/14 to 5/17/2011	Sub-teams continue drafting requirements. Late April webinar on format, concepts
Little Rock, AR AECC	5/17 to 5/19/2011	Review of Standards with regional and NERC audit Staff
Interim	5/19 to	Sub-teams continue drafting requirements based on

Meeting Location	Dates	Meeting Objective
	6/21/2010	feedback from regional and NERC audit staff.
TBD	6/21 to 6/23/2011	Review of Standards and implementation plan based on feedback from regional audit staff
Interim	6/23 to 7/19/2011	Sub-teams continue drafting requirements
TBD	7/19 to 7/21/2011	Technical workshop with invited industry representatives
Interim	7/21 to 8/23/2011	Sub-teams continue drafting requirements based on industry representative feedback [Sneak peak industry webinar in early August - ???]
TBD	8/23 to 8/25/2011	Quality assurance review with NERC staff to prepare standards for posting
Interim	8/25 to 9/20/2011	Posting for formal/informal comment
TBD	9/20 to 9/22/2011	Industry Webinar or Technical Conference?
TBD	10/25 to 10/27/2011	Respond to industry comments
Interim	10/20 to 11/15/2011	Continue responding to industry comments
TBD	11/15 to 11/17/2011	Continue responding to industry comments
Interim	11/17 to 12/13/2011	Continue responding to industry comments
TBD	12/13 to 12/15/2011	Quality assurance review with NERC staff on posting for formal comment with concurrent ballot.

Appendix 8

CIP CYBER SECURITY STANDARDS STYLE GUIDE – FEBRUARY 17, 2011

This is a Standards development style guide for the Cyber Security Order 706 Standards Drafting Team. The guidance here only serves as a companion document to the required elements of drafting NERC Standards. In all cases, the NERC Rules of Procedure takes precedence over guidance presented in this document.

Refer to the following diagram that reference the parts necessary in each requirement. Drafting guidance is given for each requirement part listed.

Requirement Parts

R1. Each Responsible Entity shall develop and implement one or more cyber security policies that include the required items in *CIP-011-1 Table R1 – Security Governance and Policy*.

Rationale: *One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.*

Summary of Changes: *[Use this section to describe any broad changes applying to multiple rows in the table or removed requirements. These changes require the same level of justification as in the table rows. If all changes can be sufficiently described in the table rows, then this section can be omitted.]*

Additional Guidance: *The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs.*

1. Introductory Requirement

2. Rationale

3. Requirement-level change justification

4. Additional Guidance

5.

6. Requirement

7.

	CIP-011-1 Table R1 – Security Governance and Policy		
	Applicability	Each Responsible Entity shall include the following in their Account Management Documentation:	Measurement
1.1	Minimum	Specify applicability to organizational and third-party personnel	Verify that specific language in policy exists that address applicability to organizational and third-party personnel
Reference to prior version: CIP-003 R1		**Change Justification:**	

8. Reference to Prior Version

9. Row-level Change Justification

1. Introductory Requirement

The introductory requirements text must be stated as:

Each Responsible Entity shall implement one or more processes that include the required items in CIP-011-1 [Table Title]

2. Rationale

EACH REQUIREMENT MUST INCLUDE A RATIONALE SECTION. THE RATIONALE SECTION SHOULD STATE:

- WHY A REQUIREMENT IS NEEDED
- WHAT ASSUMPTIONS WERE MADE
- WHAT ANALYSIS EFFORT DROVE THE REQUIREMENT (IF NOT CONTAINED IN CIP VERSION 4)
- SOURCE OF ANY NUMBERS

3. Requirement-Level Change Justification (Summary of Changes)

Use this section to describe any broad changes applying to multiple rows in the table or removed requirements.

- These changes require the same level of justification as in the table rows. Describe how these changes address a directive, interpretation/CAN topic, broad industry feedback or significantly improve the Standards.
- If all changes can be sufficiently described in the table rows, then this section can be omitted.

4. Additional Guidance

Each requirement should have guidance to describe acceptable ways to apply security requirements. Specifically, where operating environments play a factor in applying mitigation, consider documenting *how* entities can apply high-level requirements at a power plant versus a substation versus a data center.

5. Applicability

The section should be used to specify where a requirement applies as well as any exceptions based on cyber system characteristics.

- ***Impact Level*** – Specify either *Minimum* or *High Impact*. We may add a third impact level in the future, but these are the only choices at this time. Refer to Appendix A for additional guidance in determining the impact level
- ***Requirement Type*** – Specify *Programmatic*, *BES Cyber System*, or *Component*. Programmatic means the requirement applies only to having and implementing a program for all BES Cyber Systems but is not assessed at the system level. These are only candidate requirements at this time until we receive further guidance from NERC compliance staff. *Component* requirements indicate this requirement applies to individual components of the BES Cyber System.

- ***Operating Environment [Optional]*** – Specify *Control Center, Transmission Facility*, or *Generation Facility* if this requirement only applies to a specific operation environment. This means the BES Cyber System resides within that operating environment.
- ***External Connectivity Only [Optional]*** – Specify *External Connectivity Only* when the lack of connectivity provides compensating mitigation for a specific security requirement.

6. Requirement

Ask the following questions when evaluating requirements or sub-requirements:

1. Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? If these questions cannot be answered
2. Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? If so, the requirement may be too specific
3. Is the timeframe arbitrary?
4. Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

Within a single requirement, approach writing the requirement rows in a hierarchical fashion. Move down the following hierarchy and write lower level sub –requirements only if additional or different controls need to exist to mitigate vulnerability or threat and/or enhance auditability.

- Write minimum requirements applicable to all BES Cyber Systems
    - Write requirements for high-impact levels
        - Write requirements specific to authority types (i.e. TOP, GOP, etc.)
            - Write requirements specific to location (i.e. Transmission Control Center, Generation Plant, substation)

Begin with programmatic requirements, moving toward more detailed technical controls requirements with a goal of minimizing prescriptive controls. Requirements should be written at each necessary level in context of the established rationale.

5. Measures

Each requirement row should have a measure to describe specific examples of acceptable evidence that may be used 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. Use the following guidelines in developing measures:

- EACH MEASURE MUST IDENTIFY THE FUNCTIONAL ENTITY
- EACH MEASURE MUST BE TANGIBLE, PRACTICAL, AND AS OBJECTIVE AS IS PRACTICAL
- MEASURES SHOULD SUPPORT REQUIREMENTS BY IDENTIFYING WHAT EVIDENCE OR TYPES OF EVIDENCE COULD BE USED TO SHOW THAT AN ENTITY IS COMPLIANT WITH THE REQUIREMENT
- DO NOT USE “SHALL” OR “SHOULD” IN A MEASURE

Requirement	Measure
Calls for document	Require the responsible entity to provide that document
Calls for document having timing-related aspects such as "current" or "updated"	Evidence must include references to dates
Is to verify something	Include the criteria for verification and the evidence to support that the verification was conducted
Is for verification to be executed on some periodic basis	Evidence must include references to dates
Is to take an action	Include evidence that the action was performed
Is for action under specified conditions or with some specified frequency	Include evidence of the conditions under which the action was performed or a reference to the times when action took place, to support the frequency

6. Reference to Prior Version

Document any references to CIP Cyber Security Standards version 4 in this textbox.

- If no requirement in CIP version 4 exists, document "*No Previous Requirement*"
- If this is a new requirement, document "*New Requirement*".
- If a requirement row covers a broad conceptual change (i.e. covering policy references across all CIP-003 through 009 Standards), describe this change in the Requirement-Level change justification and document "*Refer to Summary of Changes Above*"

7. Row-Level Change Justification

For each row, describe how these changes address a directive, interpretation/CAN topic, broad industry feedback or significantly improve the Standards.

- If there is a source for the change, it should be stated but not quoted verbatim.
- If it is in response to a FERC Directive, state the specific directive by paragraph number.
    - In responding to the FERC directive, provide additional context to the options considered in reaching the change.
- If there are only minor changes, state *minor wording changes*.
- If a requirement row covers a broad conceptual change (i.e. covering policy references across all CIP-003 through 009 Standards), describe this change in the Requirement-Level change justification and leave this box blank.

NERC Staff will prepare the CIP reference document and FERC directives mapping from the change justification statements.

Appendix A: Guidance in Determining Controls for High Impact

BES Cyber Systems at Transmission Facilities

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

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

BES Cyber Systems at Generation Facilities

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

- **High Impact BES Cyber Systems**
  Primary Concern: Attackers using it as a launching point to high impact assets or attackers gaining easy access to a large number of facilities.
  - Controlled access to upstream networks (limit use as a launching point for attacks)
  - All passwords must be changed from manufacturer defaults on all devices that support a password.
  - Strong authentication required for all remote electronic access
  - Good ingress & egress network access control
  - No physical security requirements
  - Organizational Controls
- **Enhancements for Impact Level A BES Cyber Systems**
  Primary Concern: Attackers gaining control of single large units or multiple units within the plant.

- Physical access control and logging.
- Strong, highly controlled segmentation between individual generating units.
- Electronic access control and logging for all remote access.
- Good systems management, change mgt, vulnerability mgt on control system servers, HMIs.

BES Cyber Systems at Control Centers

Centralized data centers. Easier to apply automated security controls.

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

Appendix 9

February 2011 CSO706 SDT Meeting Evaluation Summary

13 Responses Received (1=Very Satisfied … 4=Dissatisfied)

1. Overall meeting format and structure (13 responses, Average of 1.8, Top =1, Low=3)

Comments:

- Facility very good. Location a little out of the way
- Too much ground hog day

2. Use of Webinar and phone/audio for this meeting (10 responses: Average of 1.5, Top=1, Low=3)

Comments:

- Nice having this kind of sound system
- Like having individual mic's
- Could be improved by providing the chairperson an additional monitor to avoid excessive cycling of windows
- It was particularly difficult to hear John Lim. Because John is the Chairperson, this was a challenge.

3. Distribution of timed agendas and meeting objectives in advance of this meeting (13 responses: Average of 1.8, Top=1, Low=3)

Comments:

- Some materials hard to locate or unavailable prior, but volatile process may dictate
- Info provided in a timely manner. Don't always follow the agenda
- Agendas good would like better definition sooner on what is expected for meetings

4. Sub-Team meetings in between face-to-face meetings (12 responses: Average of 2.1, Top=1, Low=4)

Comments:

- Getting to the timely content, again, seems illusive.
- We really need to get the high level minimum controls needed for low devices across all the groups.
- Not as much participation as desired
- No CIP-002-5 meetings I was aware of.
- Need more SDT participation
- The need to invite everyone on the Plus List to individual sub-group meetings hampered progress

5. In your view what improvements in the meetings and the overall SDT should be considered?

- Clear communication to subteams on tasks to be performed. I'd like to see it in writing to the whole team so we are all on the same page.
- The team dynamics are good. Ideas are freely offered and thoughtfully considered. However, the debate is often circular, returning to the same discussion over and over. Some means to limit this seems to be needed. After a point(determined by team vote) debate is suspended on specific topics.
- It would be very helpful if those who are vocal with criticism of work would themselves participate in the writing of the requirements.
- The scope of what needs to be protected has to be established. Controls can be built around the scope.