NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

April 13, 2010 | 1:00 PM to 5:00 PM EDT
April 14, 2010 | 8:00 AM to 5:00 PM EDT
April 15, 2010 | 8:00 AM to 5:00 PM EDT
April 16, 2010 | 8:00 AM to 1:00 PM EDT

Unanimously Adopted, May 13, 2010

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT April 13-16, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT APRIL 13-16, 2010 MEETING
EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 21st meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The host Jay Cribb, a SDT member, welcomed everyone to the facilities and covered logistics. Bob Jones, facilitator, reviewed the proposed meeting agenda. On Friday morning the SDT approved without objection the meeting summary for the March 9-12, 2010 SDT session in Phoenix, Arizona. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines.

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials.

John Lim provided an overview of the revisions of CIP-002 Draft Final and SDT Industry Response Document since the Phoenix meeting. The SDT discussed the following topics:

- "Immediately affect real time operations."
- Interconnections.
- Attachment 2, Item 1.6- 3 or more transmission lines.
- VSLs
- Miscellaneous topics including functions, compliance issues,

The Chair noted that since the Phoenix meeting, much work has been done by the CIP 002 Sub-team responding to the input and suggestions received. The Team sent to NERC staff a preliminary draft for their input. However subsequent to submitting the drafts to NERC, the Sub-teams produced further refinements to their drafts. The Team agreed to review the NERC comments and consider them in relation to the current draft of CIP-010. Howard Gugel led the SDT discussion of the NERC staff comments on the earlier draft of CIP-002 as well as various proposed edits, such as using the term "requirements" throughout the documents, utilizing owner/operator vs. user, defining "immediate" and "situational awareness." The SDT reviewed all of CIP 002 requirements and Attachments #1 and #2 and took a number of polls on whether to accept the proposed NERC edits.

On Friday, John Lim reviewed CIP 002 Sub-team's redline version to address some of the issues raised earlier in the meeting and reviewed the proposed language on: Definition of BES Cyber System and the definition of "immediate"; High impact rating; and Transmission facilities.

On Wednesday, the SDT reviewed the work of the CIP 003-009 Sub-teams since the Phoenix meeting (including Change Management; Access Control and Auditing; Recovery and Response; Operations; and Personnel and Physical Security). The SDT

focused first on reviewing and refining the Security Governance requirements including the proposed 9 category areas.

Wednesday evening the Chair asked Howard Gugel to prepare a sample "proof of concept" for the access control requirements to inform a decision regarding format of the standards.

Thursday afternoon the SDT reviewed each of the sub-team's draft requirements as revised and refined in the sub-team meetings on Wednesday, offering guidance on various issues raised by the draft requirements.

The SDT reviewed and confirmed previous decisions to use tables in the new CIP standards and to formulate objective statements for each requirement. Sharon Edwards presented the work to date on access control including CIP-004 R4, CIP-005 R2, CIP-008 R5 and dispersed throughout the standard as a way to highlighting the presentation of different formats. Following this the SDT reviewed three format options:

- **Option 1.** Keep CIP-003 to-009 and work from there.
- **Option 2**: retire existing CIP standards and organize the new standards by the topics in sequence from CIP-010 on. (e,g,.,Access Control could be CIP-017).
- **Option 3:** One big standard document with 2 sections CIP-010 (formerly CIP-002) and CIP-011 (formerly CIP-003 to -009). All controls requirements would be together in one CIP standard, with CIP-011:
  - R1 (security policies) addressing all topics.
  - R2 implement per table
  - R3- table for access control
  - R4 implement 2nd table (account specifications)
  - etc.

The Team following the discussion of the pros/cons of the options, voted first on each of the three options indicating its acceptability. Following that each Team member voted to support the option they found most acceptable or preferable based on the discussion and their perspective.

Format Option 1: keep existing CIP 003 to 009 in its current form maintaining its existing logical construct (may involve minor movement of existing requirements between standards)

Yes	*No*	*Indifferent/could go either way*
8	**7**	**3**

Format Option 2: Retire 003 to 009, create new CIP 011-17 grouping according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**2**	**6**

Format Option 3: Collapse CIP 003-009 into a single standard that contains all requirements created/edits by the sub-teams and grouped according to sub-team assignments.

Yes	*No*	*Indifferent/could go either way*
12	**7**	**2**

The team then voted for one of the two highest ranked options under consideration:

- Option 2: Retire 003 to 009, create new CIP 011-17 grouping according to small group assignments.
  ***Yes*=6**
- Option 3 Collapse CIP 003-009 into a single standard that contains all requirements created/edits by sub-teams and grouped according to sub-team assignments.
  ***Yes*=10**
- *Abstained from voting for Option #2 or #3:* 4

At the end of Thursday, the Team took up the format issue again. The Vice Chair made a proposal that the Team use Option 2 (which would renumber the requirements using the topics to organize them).

The facilitators polled the team on their support for the **Option #2 (multiple standards) and 7 of 16 members** were in support of utilizing this as the format. An additional member joined and the Team then tested support for **Option 3 (putting all into single standard) and 9 of 17 supported using this format.** Neither format approach received sufficient support to make an SDT decision.

The Team then reviewed and tested support for each of the following propositions:

1. Change from existing CIP numbering system? Yes- 13 favor changing (of 17 = 76%)
2. Adopt the proposed headings for the requirements as the categories whether as one or multiple standards? Yes-13 (of 17 = 76%)

On Friday morning the SDT took up the final review of format options for the informal posting document(s) in order to make a decision.

The facilitator suggested the SDT use an acceptability ranking of the two possible format options that had been discussed and debated yesterday followed by clarification of concerns to see if they could be met and a requisite number of members could agree on the format to use for the informal posting.

- **Option #2 – Requirements in Multiple Standards.** Use the Topical areas discussed on Thursday and utilize multiple standards (example CIP 010 -020). CIP 002 also gets re-numbered.
  4**=3,** 3**=7,** 2**=6,** 1-**0** *(Avg. 2.81)*

- **Option #3 – Requirements all in One Standard.** Use the Topical areas discussed on Thursday, but one new standard is posted containing sections for all topics. 4=**6,** 3=**5,** 2=**3,** 1=**2** *(Avg. 2.93)*

The 17 SDT members present then voted for their preference for posting for informal comment between the two options with the following result:

- **Option #2** *(multiple standards)* **Yes= 6 (35%)**
- **Option #3** *(single standard)* **Yes= 11 (65%)**

The SDT agreed that while this decision to post for informal comment has a majority support (65%) but not the super majority (75%) of the members called for in the decision rules, the Team is asking for industry comment and input on the formats through the comment form before finalizing a format to present in the formal comment draft in July, 2010. The Team discussed that this approach is consistent with the spirit of the following consensus rule provision: "In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team."

On Friday the Chair reviewed the schedule, assignments and next steps for the SDT to produce a final version for posting on May 3, 2010. Joe Bucciero will lead, with assistance from Howard Gugel, preparation of the draft of comment form with information provided by each of the Sub-team leads. A question will also be added based on the discussion on the format of the CIP Standards. The SDT will need to begin creating an implementation plan for posting in July for formal comment. A small group of SDT members needs to be formed to provide some framework for discussion at the May meeting (in Dallas) and to answer any questions at the May SDT Workshop in Dallas. Scott Mix will be looking for individuals to work with him to prepare the Implementation Plan, and this will occur after May 3. The SDT agreed that the cover letter for the informal May 3 posting of the draft CIP Standards should speak to the SDT's philosophy on implementing the plan. Jackie Collett, John Lim and Doug Johnson agreed to work with Scott Mix on developing a draft implementation plan.

The Chair reviewed and the SDT agreed on the schedule of activities from Monday, April 19, to posting of the draft CIP Standards on Monday, May 3. The Chair and Vice Chair and the SDT thanked Jay Cribb for his excellent hosting and Southern Company for the great facilities.

The meeting adjourned at 12:00 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CYBER SECURITY ORDER 706 SDT- PROJECT 2008-06
21ST MEETING SUMMARY

April 13-16, 2010
Atlanta, Georgia

I. AGENDA REVIEW AND WORKPLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 21st meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Jay Cribb, a SDT member, welcomed everyone to the facilities and covered logistics. The Chair reviewed the following meeting objectives:

- Review the revised CSO 706 SDT 2010 Work plan and Schedule
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and the May 2010 Technical Workshop
- Review, refine and adopt the Draft Final CIP-002-4 for industry informal comment
- Review, refine and adopt the Sub-Team Security Control Requirements draft for industry informal comment
- Develop related CIP 002 and Security Controls Requirements Guidance Documents
- Agree on next steps and assignments

Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Friday morning the SDT approved without objection the meeting summary for the March 9-12, 2010 SDT session in Phoenix, Arizona.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

B. Workplan Schedule Review

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials. Joe Bucciero suggested the SDT might want to review this overnight and take up first thing on Wednesday morning.

II. CIP 002 REQUIREMENTS

A. Overview of CIP-002 Requirements

John Lim provided an overview of the revisions of CIP-010 Draft Final and SDT Industry Response Document since the Phoenix meeting, noting the following:

- R1 changes: "Uniquely" changed to the adverb "discretely,"
- Member comments and suggestions included: take the adjective out. Consider "discretely" "distinctly" May not need this word. The call is document all; this may be "lawyer bait."
- R2- "appropriately: added.
- Attachment 2. Used terms defined in the glossary. Didn't change thresholds. 1.2- struck generation. Threshold too high. 1.6- before had separate criteria for protective systems. And protected at 350 or higher without any qualifications. Covered all substations at 350 KV. Not intended. Merged with 1.11 with 1.6.
- Medium: thresholds lower than before. Protection systems with 3 or more lines. Rest fall into the medium.
- Member comments: 2.5- no fax systems- everyone is high? This is an oversight.
- Low Impact: added to be consistent with high and medium.

SDT Comments on Overview

"Immediately affect real time operations."

- Short range planning impact issue? Other situational awareness but not in the "immediately affect real time operations" language? Does it include next day planning?
- John Lim noted that they didn't have a consensus in the group on this.
- "Immediately"- what does this mean? Week, day, now? Are they needed.
- Maybe we should distinguish from planning and real time operation.
- Since you refer to operations planning in part 1. In part 2 need to apply to operations planning.
- Look at beginning of Attachment #1 language.
- Attachment 2- 1.1- "facilities – why combine generation facilities?
- BES cyber system is subject which covers shared cyber system.

Interconnections.

- Texas- lower requirement for ERCOT? Why a separate requirement for ERCOT? Different size in terms of megawatt capability and mode.
- Why have spinning reserve requirements higher in ERCOT?
- This focuses on the Texas and Quebec interconnections.

- Did SDT December posting allowed for regional variation? Not by regional variations but by interconnection variations. Numbers come from category 3 events.
- Definition of control center? Lower threshold will bring in more things. E.g. 1.7 medium- primary and backup control centers? Are these defined? How are they distinguished from control centers? Shouldn't assume everyone understands these terms.
- Work is being done on a NERC back up facilities standard. Went through initial ballot but didn't get support on that proposal.

1.6- 3 or more transmission lines.

- 1.6- what was technical basis behind 3 lines?
- 1.6- 3 or more transmission lines? Individual connectors? What about DC circuit with 2 lines on the tower? One transmission line or referred to as conductors or phases.
- In the context of transmission planning studies, 2 or more would be ridiculous. 3 or more is a good place to draw a line.
- We have redundant subsystems. 3 line threshold may be too low some companies.
- 5 transmission lines would be hard to justify for a national standard. 300 kv above and higher.
- Multiple entities have asked for the technical basis for this. Need to respond if we leave it at 3.
- "Or that remotely control a BES asset with a high impact rating" Asset= facility? Hardware?

VSLs

- VSLs measure R1 in terms of how many you miss. Assumes auditors know the right total. How will this be computed. This is defined by the entity. These are squishy number to begin with.
- Auditors won't use this. This is not looked at part of the audit itself. Use only when there is an alleged violation. After a potential violation an investigation is conducted to confirm a violation and the circumstances associated with a violation. Then someone comes to do analysis what the count should have been.
- Every requirement must have a VSL or FERC won't accept.
- We can make this a number vs. a %. 1, 2 or 3. Have not been identified more than 3 high.
- Previous VSLs had numbers. Some entities have suggested 5 could be a small number.
- Don't see the difference between 1 and %. Issue is entity is identifying the cyber system. Investigator and entity work together to define- a number or % calculated.
- Are we spending too much time on VSLs? Difficult to correlate the auditing fine and the VSLs. What value is added by debating VSLs *ad naseum*.
- What about using "misidentified"
- Get rid of % but develop better definition of the BES cyber system

Miscellaneous

- Is the whole functions area a mush?

- BES cyber system identification is up to the entity. Entities will appropriately draw the line in different ways.
- This is where we need NERC compliance to weigh in to provide advice to the SDT.
- Concrete recommendation: Eliminate line 1 on chart since it is untenable since you can't calculate a %.
- This is not an audit tool to determine if you have met the requirement.
- Requirement is to identify all BES cyber systems.
- First step is to find if you find a BES cyber system that wasn't identified. The investigator will develop the list.
- Add "Additional"?
- From #2, on it presupposes you have a list.

B. NERC Suggested Edits for CIP 002-4 *(Including Maureen Long and Dave Taylor)*

The Chair noted that since the Phoenix meeting, much work has been done by the 002 Sub-team responding to the input . The Team sent to NERC staff a preliminary draft for their input. However subsequent to that the Sub-teams produced further refinements to their drafts. The Team agreed to review the NERC comments in relation to the current draft 002. Howard Gugel led the SDT discussion of the NERC staff comments on an earlier draft of the SDT.

SDT Comments and Polls

Definitions section.

- Functions sentence should remain.
- List doesn't have a proper introduction in Dave's edits.
- Computer systems themselves are control centers, not the dispatch arena etc.? Not supporting
- In the field- this is a control center.
- Is there a something out there- is a computer or a programmable controller.
- This is the first time the SDT is using "computer systems"- will be confusion on this.
- Remote data collection equipment as well.
- A control system vs. control center? Leery to tying back to computers.
- Does fix some physical security if only around computer systems.
- Tied back to EOP 8. Do you need to define control center?
- Go back to original wording. Not trying to define BES cyber system.
- "associated"
- Propose striking second sentence.
- EOP 8- strong linkages with other standards raise double jeopardy issues.
- **Retaining the SDT language:**

Y	N
15	0

- **Add "Functions that support"**

Y	N
15	0

- "typically" in the second sentence)-
- For a definition, we should remove the second sentence.
- "At a minimum"? No.
- Are we removing reference to real time operations?

- Retain the 2nd sentence and remove "typically"?
- Delete: "listed below" in first sentence.
- All agreed. 002 Sub-team will follow up with these changes.
- Purpose addition. OK
- "including the date the identification was performed"? OK no objections all agreed.

R-1

- The 1st thing NERC suggested was to make 1 and 2 a single requirement that has 2 parts.
- If you don't put criteria on correctly but come up with violation. If you have list and criteria. Violation for either part? Or if stick with separately changes for R1 and R2. This might eliminate struggles with VSL statement earlier.
- R1- from "all " to "each"? "One or more" If we use R1. Why not make R3 subset of R1?
- NERC had advised against doing sub-requirements?
- Sub points not sub requirements. All one requirement. This is very confusing.
- Leaning towards keeping current structure.
- This format is being used in other standards. Filed with FERC. May be obligated to use. Either way may be acceptable.
- Benefit to sub numbering format. Keeps together things by. Sub numbers help clarify the numbers intent.
- In favor: of **Sub numbers option**

Y	N
7	9

- NERC's suggestions on R1. Requirement is to "identify" and "all" vs. "each". Identify and document each.
- **Should we accept the NERC R-1 recommendations?**

Y	N
1	16

- **Delete "Document"**

Y	N
2	15

- **"Each"**

Y	N
5	12

- Make sure you identify all cyber systems. Indentify suggests uniqueness.
- "Each" identify something- each in a set. Discreetly" problems with how you document. E.g. on multiple lists vs. 1 list.
- What do we mean by BES cyber system- box or applications? What does discreet"
- **Delete "Discreetly**

Y	N
16	0

- Use vs. own (regardless of whether you own it). E.g. I.d. 3rd party tagging application. Have to do something about. "Owns not uses"

- Note that asset owners and operators make for a big difference. Possibly use: "Owns, operates or owns/operates"
- Owner knows what the equipment is but the Operator may not.
- BES cyber systems that execute or enable?
- **"Owns" vs. "uses"**

Y	N
13	4

- Its got to be ownership or else there will be big headaches. Asset means ownership.
- What about jointly owned? Agreements/contracts would address those kinds of issues.
- SDT should lock it one way or another. There will be fewer exceptions with owned than "operates."
- To enable functions. Applicability is solved earlier. This is not the best place to deal with this. Applicability to the standard. The entity will resolve, not us.
- Leaving executes and enables?
- Taking out is not appropriate- Whatever we decide. It will bring comments. At least it is in the open in the informal comment process.
- This is not a new issue. There is joint ownership now under current standards. We operate generation for other. It all comes down to money.
- **"Own" (2nd poll)**

Y	N
11	6

- Figure out what we need to do with joint ownership. Technical owners vs. lease holders.
- Discreetly identify- make sure you can't have things in two cyber systems.
- There is no way to document if you haven't identified. Is this idea redundant?
- We will need to do better on documenting guidance- for industry.
- True requirement is identification. Document is the measure.
- "Appropriate?" This doesn't read well without this word.
- But "appropriate"- doesn't identify anything.
- Can we move benefits to reliability to a guidance document? No, benefits to reliability is needed for each requirement under NERC's current approach.
- **Strike "appropriate"**

Y	N
14	3

- R1. Is the last sentence on the objective superfluous language?
- Breaking out the objective of requirement offers great value in knowing what the objective was in terms to later determining intent.
- NERC's requirement is to set forth the "benefit to reliability." You need the who what and why set out in the requirement.
- Would it be possible to pull out separately? It is confusing to read. Are we bound by format?
- Could change wording, "for the application of security requirements and controls to BES cyber systems."
- SDT- consensus- ok.

R2

- John Lim indicated he believed the sub-team would not have problems with changes suggested by NERC.
- The SDT accepted the changes.
- Should we require "categorize and annually re-categorize."
- Delete re-categorize?
- "Annual" is better used in the attachment.
- **Delete "Re categorize" SDT Consensus= Yes.**
- "and document such categorization for" OK
- Missing a date here? Add here "including the date the identification was performed"?
- Will we have to put into every requirement?
- Look in measures- lists have to be dated. Have to tie this back to the requirement.
- Remove this language from the measure and the requirement. Y 16 N 0

R3

- Do R1 and R2 once. R3 from now on keep it up to date.10 years later you missed a system on the list. Do you violate R3, R1 or both?
- If you never made the change, then you missed it the first time.
- That is why the sub-team added "that it owns or operates "
- What if it is change because of a storm, not planned. "Emergency changes"?
- Concerned about consistency as we go through. End each with the benefit piece. Look at the different wording on R1, R2 and R3. Make consistent. If benefit the same, use same language. R1- to categorize
- Just voted down "owns or operates." Should we delete here? Want to monitor for changes.
- Planned vs. unplanned change. Have to keep the list fairly static. Changes in a planned way so you know to change the cyber system.
- Planned/unplanned—"planned"- triggering issues. May need to look at this some more.
- Is an annual refresh missing where you look at categorization to make sure something didn't happen that you missed?
- "Reviewing the categorization of the BES cyber systems"
- Remember these are minimum requirements. Do we want to state annually. Or leave it up to entity (best practice). If you have a planned change, you have to revisit it. People can revisit anytime they want.
- Can you have a change not specifically planned? To take a line out they have to do some studies to figure this out. This doesn't happen spontaneously.
- **Delete "or operates" yes. All**
- Transmission owners vs. operators- is a problem. R1 has it as "owns."
- Every one else who is a transmission operator. R1 and R2 have to identify assets (probably a control center).
- Categorization- if control center controls a high impact high asset, high impact control center.
- If we already have covered applicability, is it appropriate to put into requirements?
- **Delete "planned = no, All**

- **Add" "<u>the identification and categorization</u>"** Yes All
- **Add " annual review"? "Every 12 months or as …"** Y N
  1 16
- Comes up in R1 and R2- got rid because no reliability benefit.
- The requirement to notify changes to others is not here any longer?
- That is because the BES cyber system is categorized.
- Sub-team Ok with Dave Taylor's suggested edits.
- <u>"to the portion of the BES" ? OK</u> Planned changes for my stuff only.
- "Periodic reassessment?- CIP 002 sub-team dealt with.
- Other changes: calendar OK
- Difference between requirement and controls. Control objective statement 800-53. Writing requirements. Are we authorized to write controls? Source documents are controls based,
- **Use the word <u>requirements</u> throughout documents. All Agreed.**

Measures

- Delete discreetly? Yes, All agree.

Compliance

- Note that data retention language and the audit periods (3 or 6 year cycle). Gap of compliance only keep data for the year not the last audit. Need to keep data since the last time audited.

Attachment 1

- **Scoping statement important- place it first? Yes** Y N
  13 4
- Make this the first sentence?
- Since "real time" was added NERC staff struck the purpose paragraph.
- "Operations planning horizon" ? Do we want to include this in addition to "real time"?
- Planning could affect real time as well.
- This doesn't appear in any R, or attachment 2. List of functions only.
- Reconsider operations planning horizon in all requirements?
- When define the functions could take place in real time or in the operations planning horizon.
- **Reorder the 2 paragraphs? No** Y N
  3 16
- **Delete ~~"these functions take place in real time or operations.~~ Create a single paragraph**. **Yes** Y N
  14 3
- If you delete the above you will have to deal with word "immediately"
- Day ahead? Marketing term.
- Take out planning horizon?
- If you pick wrong units, in real time you will figure out.

- What we are after here are control systems. Protect- 1 and 0s turns into action out there.
- **Delete ~~Immediately ?~~** Y 11 N 6
- Initially defined "immediate" within 15 minutes"
- Real time? 1 hour or less in the NERC glossary. Upper case or affects the operations within 15 minutes.
- Need that kind time frame. We do need to maintain it. If you aren't specific, may put security controls where you don't need them.
- JVB: time frame- affecting real time. Leave immediately there and have real time (lower case).
- Further qualification? Is it and, and/or?
- Intent is the be "and"
- **Delete "further qualifications?" Yes** All
- Is "Immediate" related to ability to act?
- Concerned there could be other cyber systems that don't have immediate affect. The ones of greatest importance, at a minimum, should be protected- this should to be clear.
- **"Can have an immediate effect"** **Yes** Y 14 N 3
- Need a definition of immediate? "Faster than a human reaction"
- e.g. Immediate access revocation- 24 hours.
- Near term.
- What about adding: "only those that have the capability to monitor or control real time operation of the BES"
  Concerned about "monitor." State estimators replacing what you are monitoring.
- "respond" vs. control.
- Is it clear that it control?
- **Support for single reworked paragraph. Yes** Y 17 N 0
- "Dynamic response"- editorial accept. OK
- "Cause a condition" vs. "cause a reaction"? Any difference?
- "Balancing load and generation." Ok
- Controlling Frequency
- "which ensure real time"?
- Cant control without real time. Don't need the clause.
- "Controlling Voltage" editorial accept. OK
- "Managing constraints" editorial accept. OK
- "Control and operation" editorial accept. OK
- Restoration of BES- editorial accept. OK
- "Necessary" should remain.
- "Situational Awareness"
- It is partly a operations planning action?
- Contingency analysis, close to real time (not a day ahead).

- Delete “anticipate and plan”?
- If you take this out and you take out RTOs.
- Solve by eliminating “~~and anticipate effects of planned and unplanned changes to conditions.”~~?
- Take “current” out of it? Immediately affects situational awareness?
- Only reason to use this clause is to scope this down. Addressing concerns that “this applies to everything.”
- “Assess the condition of the Bes necessary for real time operation.”
- Control and operation and situational awareness.
- Difference between monitoring and assessing.
- control and operations- pure SKADA status of components. Situational awareness.
- Assess the current and anticipated operating state (or condition) of the BES?
- Is there different information used to assess the current vs. evaluate what the future?
- It can be data not from a real time environment.
- Day ahead studies, state estimation. Don’t want to get to other studies being done.
- “near term”? data collecting is real time.
- Current, expected and anticipated
- **Situational awareness: activities actions and conditions to asset the current expected and anticipated state of the BES.** ***As revised*** Y N 15 0
- Inter Entity Coordination and Communication
- Active coordination. Communication is the action.
- Coordination of real time operation.
- Add, **“real time coordination”** Yes. All agree.
- Tie to attachment 2? General comment.

Attachment 2

- (“As determined by….”) Maureen Long/NERC suggested a determination.
- “Responsible entities”= functional model entities. We are using this. She has injected this back in. e.g. 1.1 generation operator doesn’t have a role in this.
- “Operations planning”- SDT decided to take out yesterday.
- 1.1- Generation facilities- (as determined by the Generation owner or the generation operator”. Might be at times the generation operator
- This parentheses might be not needed.
- Doesn’t clearly identify shared facility. “if using a shared BES cyber system”
- If he has all BES cyber systems.
- Non-shared system will not be connected with each other.
- “Shared or connected Cyber systems”
- That would be everything in the system.
- “Each BES cyber system that either singly or in combination. **Yes** Y N 13 0
- May not be as clear.

- Remove the rest of sentence (" ~~or more in Texas and Quebec interconnections~~")
- BES cyber system affecting a plant bigger than 2000 MW- everything in it is high impact.
- Each BES cyber system?
- "would" this is a conditional word. That ~~would~~ immediately affects
- That has the capability to immediately? "Has the potential to"? "Can have an immediate effect" (from yester day)
- **Each BES Cyber system that can have an immediate effect on real time operations"**
  All agree.

- This came from a NERC document. Disturbance report Categorization criteria. Done in 2009.
- ERCOT has higher contingency reserve- less than ½ of reserve. Lose 2 units bigger than 1000 MW.
- Engineering analysis language was in December 09 posting.
- Arguing the 1000 MW number
- Any way to ask Planning Committee regarding this issue.
- SM: "good enough to post" to get industry comments back. Leave something in. If you assume 2000 is appropriate for east- % of size of interconnection.
- Impact of loss of MW is the focus.
- **Remove the rest of sentence ~~("or more in Texas and Quebec interconnections")~~**

Y	N
8	8

- **Remove?**

Y	N
13	3

- **Strike 1.1 and look at 1.3 and go with contingency reserve. Defer, for now. Get feedback from the planning committee.**
- **All OK**
- We need a criteria. This is key. Used the disturbance report as basis. What our basis for this concept in 1.1?
- Few generators with 2000 MW – few are high impact.
- E.g. 3 or more transmission lines
- Move to medium vs. dropping?
- Support this. Contingency reserve. We've discussed before. Agreed to leave them in.

1.2
Sub-team ok with NERC edits/additions. SDT ok.

> Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Reactive Power capability of 1,000 MVAR or more in Eastern and Western Interconnections and 500 MVAR or more in Texas and Quebec Interconnections. (As determined by the Generator Owner or Generation Operator, Transmission Owner or Transmission Operator)

1.3 Contingency

- This is an annual reassessment issue
- List of issues for 002-
- Including operator. Why not "as determined by the asset owner." Not clear here.
- Refers to owner of BES cyber system. Put clause- after real power capability?
- Referencing Mod 24 and 26 testing and verification standards. The concern with linking together is possible double jeopardy. Justification in mod standards for doing both. Operator doing verification and Owner doing the setting.
- This may be an across the board issue.

Generation Facilities, singularly or in combination, (if using a shared BES Cyber System), whose aggregate rated net Real Power capability, as defined in 1.1 above, exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. (As determined by the Generator Owner or Generation Operator)

1.4

- John Lim questioned if the proposed edit is correct.
- "designate" "as designated by". Balancing authority not always the one making the reliability decision.
- Could be a number of entities.
- Unless this is universal, should be these be in at all.
- Propose striking parenthetical.
- Balancing authority- ERCOT e.g. balancing authority. But there are several entities in other places.
- "all reliability coordinators" ?
- "planning coordinator."?
- Who has a generation facility. They know what contracts/terms for their facility. Shouldn't be who is determining. Person with the asset knows.
- Some may be good or not. Possibly delete all.
- You can't have reliability without a review contract. Compliance auditors know if they have in terms of contracts
- Strike throughout attachment.
- Transmission facilities are named. Scoping built in with those words vs. entity type.
- **Strike all parenthetical**.

Y	N
14	0

- 2.7 "or that remotely control a BES asset with a Medium rating"
- 2.5 "including FACTS devises? All high impact or insert language there. (including flexible .)

C. CIP 002 SDT Discussion of Open Issues and Follow Up

- Dave Taylor's VSLs comment (15% high number? Came out of guideline for VSLs.
- Purpose reference to 003-009 will be adjusted after security controls
- Sub-team will go through the measures to ensure they are consistent with the requirements as revised.
- 1.1 and 1.6 in Attachment I.
- "Immediate"
- Annual or periodic
- 1.5. 2.4 Medium- 3 transmission lines right criteria? Where is the right number and what is the basis for that?
- 1.7 transmission facilities. FACTs devices added. Flexible AC Transmission Systems.
- Include "protection system " associated with transmission facilities? In IROLs? What is the reason it is included?
- Added to criteria for threshold for transmission-
- Looking now for consistency.
- In medium added a clause regarding protection systems 300 KV.
- Protection systems added to l.7 (including their associated Protection Systems) Sub-team will resolve how to reference this.
- Control center definition resolved? Yes.
- Is there a cyber component of systems that are not special systems? Yes.
- Retirement of term cyber asset? SDT will need to decide whether to retire.

D. Final CIP 002 (010) discussion

On Friday, John Lim reviewed CIP 002 Sub-team's redline version to address some of the issues raised earlier in the meeting and presented revisions on CIP 002, which were documented in the latest version of CIP 002.

Definition of BES Cyber System + definition of "immediate".
Rather than another definition, the Sub-team proposed to focus on the BES Cyber System definition and added "within 15 minutes" within the BES Cyber System. If the effect on reliability is within 15 minutes then the item is a BES Cyber System. This gives a finite time.
SDT Comments

- Does this include protective relays? Yes.

High impact rating
SDT Comments

- Is this – reserve sharing usually goes up – is it intent to move more in or more out?
- Parenthetical – I understand it but not sure anyone outside this team will understand it
- Meant to qualify or explain as a shared BES cyber system

- This doesn't make the "shared" clear – may need an explanatory box as opposed to a parenthetical
- Delete front end of the parenthetical
- Meant to clarify what it is meant by combined operation
- Using singular or in combination
- Team will work on exact language – concern noted

Transmission facilities

- This language helps but still concerned about parallel lines
- Changed to 4 to address terminal stations
- The parallel lines are a concern in our area
- Not sure we can address in the standard itself
- Other changes are on the medium impact – will need to address some of the comments and changes in the high impact discussion
- 1.14 - Consider moving transmission operator functions to the front of the statement for clarity – agreed
-
- Jackie Collett's email offers a rephrased version of earlier discussion
- May need to take out the first "or" from restatement
- Too long a sentence and confusing, so she tried to break it into two sentences and add punctuation to help clarify.
- Programmable electronic device – don't you want to say processor somewhere? No, working on programmable devices
- Worried about phrasing – if send info to cell phone does that phone become a BES asset – do we need the phrase "on data display"? It is the use of the data displayed that is the problem, not the display of the data.
- Semantics that may cause more problem to correct – need to give it more thought to see if can address without creating more problems
- Shouldn't we pull in language from Attachment #1 to establish what the BES system is?
- Cannot refer to an outside document within a requirement.
- Trying to write the scope into the requirement? Careful, need to keep it general
- May be getting too specific to say data used by an identified operator.
- Would removing "data" address the question? No we are also protecting the data
- What are we adding with the additional statement about BES condition or disturbance? Pull out of here and put into
  Attachment #1 – we are trying to say the function in two different ways and it is confusing.
- But, again we cannot refer to a separate document.
- Shouldn't try to put any of the functions in – gets too messy.
- "relied on to make real time operations decisions"
- Propose taking suggestions to the subgroup for refinement.

- Consider two short definitions – one for BES cyber system and another for cyber system
- Rest of 002 Sub-team will review on Wednesday.
- In definition of situational awareness – when is the anticipated state? What period of time? See qualifier at the top of the page

III. CIP-003-009 REQUIREMENTS (CIP 011)

The SDT first reviewed the Security Governance draft approach and the progress made for each to the Sub-Teams since Phoenix. The Sub-Teams then met on Wednesday to continue drafting work and presented the draft document on Wednesday and Thursday.

A. Security Governance Sub-Team report

- Jon Stanford presented document noting his sub-team had received statements from only two sub-teams- looked to other sub-teams to get their requirements.
- What is the mechanism to get into 003.
- R1: 3 sub bullets. Scope of applicability to organizational and third party personnel
- Security roles and responsibilities
- Identification of a single senior management official with overall responsibility for leading and managing implementation of requirements within these standards.
  - Provision for emergency situations? Address in recovery and response? Policy objectives
  - Annual review and approval of cyber security policy assigned pursuant to R2. Not in agreement.
- Manager responsible for implementing. "review and approve" – suggesting an org structure.
- Separation of duties issue.
- Delete 1.5 out.
- Clause " with authority" is not in current draft.
- 1.3 "with overall authority and responsibility."
- Topical areas removed. Not addressed in policy document? Requirements by topics- replacement for part of your security document.
- From 2 on- cover policy statements by topics. You to have a plan here, topic sections will describe what's in the plan. Took topics out- carry over from Federal thinking. They will be requirement statements.
- 1.3 annual review? IN the base statement in R.1. Require the REs to annually review.
- FERC wants the same person to know about.
- 1.3 overall authority and responsibility.
- Consistency. In CIP 002- eliminated annual review. Initial and upon changes vs.
- Annual review in policy statements and cover it globally.
- Program review if global

- JS: some requirements for annual review of a plan.
- SM: Double jeopardy- how write language of policy in 3 vs. procedures and plans in other standards. Don't link too tightly together.
- Annual review- different from CIP 002 annual review issue. What would be the triggering event? At policy level. Annual review catches what has happened in year.
- Feds- bi-annual review of high level policy document. At least every 2 years.
- Annual review is practiced in the industry. Good to put in as a requirement. Don't need to say who does. Senior manager should approve?
- Tie to responsible entity
- Some have single policy, some have more than one policy. Separate policy for NERC CIP.
- Presupposes they approve.
- Interpretation questions. Single senior manager. Per responsible entity. A company could have different officials. Each functional model entity.
- Double jeopardy issue we can't solve
- By functional model- have many registered entity. Let the organization decide. Can be the same or different.
- CIP Cyber security policy focus here. Consistent with version 3. Not broader security policy.
- Senior manger was to insure accountability. $1 million a day. Why special requirement. FERC directive.

R2

- 4 sub numbers.
- Shall develop a system security plan for each BES Cyber System that: 4 bullets.
- What is the need for this? Comes from a federal space. We may not want a system security plan? (describes operating environment for what you are protecting)
- List of BES cyber system out of 002. Where is the best place to document. Some requirements provide for plans.
- All documentation required. If it is spread around, then take this out.
- Security plan not only in federal model. Becoming a standard way to define system security.
- Maybe as guidance- accumulate documentation and place where makes sense.
- Make auditing easier if they have 1 place to go to for each system. Easier to see how came about. If you provide this.
- Notice requirement for a document for each BES cyber system regardless of level. As written for each and every one. Auditor needs only finds a missing document to be in violation.
- Isn't a new challenge for large multi-nationals. "Real time" operations in CIP 002- number of different REs involved. Compartmentalization. Entergy- single VP- fossil nuclear, distribution, etc. fiduciary presidents of 5 operating companies in 4 states. If divide up may not have security.
- Program plan- describes things you have to address. IN areas such as access control systems
- If came back to command and control fabric- systems that do that. Organization "shall". Have a program plan for how to attack each of the technical area.

- Security plan for each BES cyber system.
- CIP 006 physical security plan that needs to get added.
- Keep this a much higher level.
- Why look at BES system first and then at BES cyber system.
- This could create nightmare scenario.
- Security plan that addresses the following for h/m/l. Not at each cyber system level.
- Too onerous. Have security requirements for low impact systems. Security plan doesn't add much to what you are already doing. Have to document environment to demonstrate compliance. Think of
- For high impact assets need this level of documentation because of their important. Specific plan. At low level, generic plan how we address these as a whole. Not as onerous.
- Program plan approach?
- Other requirements may lend themselves to this.
- Coalesce all the plan requirements into a program plan by topic. High assets- security plan requirements.
- Program plan a good one.
- Incidence response and restoration plan. Just mentioned. Cover exclusion for emergencies.
- Details of what is in the plans in others requirements.
- "The security for each BES cyber system will be addressed in a security plan.
- Responsible entities came from markets. Shakes down to 3 organizations. Operating unit.
- Model for policy statements- in R3.
- Each responsible entity shall:…..
- Program plan-- take each of the topical areas "BES cyber system connections" DHS Control system connections.
- Authorize and document external connections. Only those authorized are in place.
- Revise R2 to include topics.
- R4 down- talks about plans- info protection plans.
- Codify details of procedures.
- Rework R2 and put a program plan approach.

R3

- How is R3 a policy? Embedded in controls document. Pull out of here?
- Won't need this if we take program plan approach.
- **R3 is redundant**. All Agree. JS will remove.
- 3 Rs.- in 003 (manager, program plan)
- E.g. configuration management plan- vulnerability assessment etc. Will these be set out as topics?
- Keep simple, not require multiple plans, but set out the topical areas.
- Probably won't need topical areas going forward.
- Program plan approach simplifies. Collapse these down.
- "Policy"- what do we mean?

- "shall language"- requirements framework- everything is a shall. If you are getting into procedures, attributes. If you are talking about topics.
- E.g. Personnel screening process. Shall have this. Procedure on how implement.
- Have to be careful- shall includes- have to have a policy. These are the areas you have to address in the policy statement about the CIP standards.
- Recovery plans and incidence response plans- not policy? Require you have one and have to do it. Develop and implement the plan.
- The plan must contain the following- e.g. recovery plans must contain….
- E.g. CIP 008 and CIP 003 statement- possible double jeopardy?
- How to deal with CIP 003, if you don't have that requirement as a low? Low impacts that don't require a response plan.
- 1 approach – policy statements you will do access control, you will.
- 2nd approach- you have to have a plan for all these things.
- Current CIP require plans where you may not need plans. Create compliance activities that have been necessary for enhancing security.
- All in a single table- do everything in a table. Policy should address. E.g. 4.3 include applicable controls specific in Table 1 Information Protection Controls.
- CIP standards are topically light and DHS are topically heavy.
- Agreed on program plan approach. Don't know where policy will go. Then come back with a proposal.
- Easy to write a double jeopardy requirement. Just to create policy statements. Policy statement you have to have recovery plan. CIP 008 and 009- plan contents. Measure for the policy- policy statement. If measure in CIP 003- you have plans to support the policy. Draw a line between requirements for policies and writing plans.
- Sending over the plan? Annual review and updates in CIP 003. CIP 006 here is what plan contain.
- This is a global question. Handle annual review in 003 or in the subsections?
- Requirement- policy statement that addresses recovery plans. Go to CIP 8 & 9 about content of plans.
- In requirement- state what the policy must address. Guidance document to be developed what the thought was behind the requirement.

R4

- R4 a problem? Looks ok.
- R4- e.g. where you are putting in requirements for the contents of plan. Here just say you have to have a plan.
- If this creates a double jeopardy problem would have to roll up into R1.
- Address the topic of information protection.
- Read it as a family of one. Why not make it one.
- Tie up topical areas in R1. Policy statement to be made in topical areas will be made in the sections.
- Does this raise double jeopardy issues?

- Puts all high level requirements in one place- shows accountability.
- Asking whether we need policy statements in CIP? Every requirement in standards is a policy?
- In practice, that is how they are written today. Current 003- policies should address all requirements.
- Doing it by topic. Not as granular as current 003.
- Placed some of these info mgt requirements here in the last week- they tie the policies to the program elements. Put things together that belong together.
- Why not put under a single standard?
- Put all tables in a single standards
- Take outliers and make them standards themselves.
- Existing format- CIP 003 policy for this, implemented in CIP 005 .
- If we change into one standard, we will hurt ourselves with the outside world.
- Move to their own standard. CIP 007 single requirement about access control.
- Standard- talks about access control (physical or otherwise)
- Does NERC have a definition. CIP 006 physical security plan. CIP 004 cyber security control training program. Do we need to get one?
- Use the same word across all standards.
- What do want to call this? "Program" is what you are doing.
- Collect all the topics together. Figure out how to put together as a team. Plans, Programs,
- 002 about scope. 2nd is about governance- management requirements. Got to have a policy and a program to address different subject areas. Outliers- are common to others, e.g. access controls. Policy can be simple what is important are the plans, woven together under management oversight.
- 003 umbrella standard- 4-9 addressing in more detail. Jumping off point for more detailed to follow.
- This standard is skeletal- areas management.
- Compartmentalized- to some degree will be necessary.
- Plans and programs- different disciplines use the same words- physical guys call things plan. What we mean is program and not a plan.
- If it doesn't lend itself to a plan.

B. Quick Update on Sub-Team Progress since Phoenix Meeting

The CIP 003-009 Sub-teams provided progress reports on work since the Phoenix meeting and then met in small groups until mid afternoon to draft or refine their requirements.

1. Change management.

- Areas- CIP 003 didn't fit into oox standard.

- Coordination- low/medium/high impact and connectivity- environmental differences? Didn't have many.

2. Access control and Auditing

- Sharon Edwards noted the excellent contributions of Jeff Hoffman and Frank Kim
- Got input from NERC
- Open issues- password measurements.
- Review what NERC offered.

3. Recovery and response.

- Scott noted good progress made and acknowledged Tom Stevenson's help and has reviewed Maureen's suggestions.

4. Operations

- Jay Cribb report that the Requirements are in good shape.
- Work needed on objectives and measures
- Coordination- ESP access points. Electronic Access Points- defined term – happy with

5. Personnel and Physical Security

- Doug Johnson reported that they have reviewed Maureen and/Dave's comments
- CIP 004. Get some policy statements over to Jon Stanford- addressing physical security and training and physical risk
- Do we still have an electronic security perimeter?
- What we have been doing- we have a word doc with a list of requirements. Get that into a real document.

C. CIP 003-009 Sub-Team Requirement Review

1. Governance

Jon Stanford presented the changes made to CIP 003 offering the following points:

- 003 can become 010
- Edited R1- adding the 9 subject areas (1.4- 1.12)
- R2- Each responsible entity shall implement the requirements specified in Table 1 (Subject Area XXX here)
- R3: Each responsible entity will implement the requirements specified in Table 2 (subject area xxx) in order to (benefit to the BES here)
- Can link VSLs to requirements

SDT Discussion

- NERC staff recommended retiring existing CIP standards and start afresh with CIP 10. Some cross e.g. vulnerability assessment is in 3 areas currently.

- Allows to quickly look through and make sure not requiring same thing in 4 requirements.
- We would need to explain- here's the map from the old and the new ones.
- Another benefit- requirement language will be simplified. As standards evolve- you'll modify the table not the policy making it more adaptable for future.
- Don't have to have a requirement that says "develop a plan"- avoiding circular logic.
- There is 1 requirement for each subject area? Will have own VRF? Everything in that Table will have the same VRF. Table will in essence- be the sub requirements.
- If we want to differentiate VRFs, we can develop multiple requirements.
- Implementation plan that will need to go along with this. If 1 standard. New implementation for a full standard.
- This will help out with the implementation plan.
- Version 4 and dates
- CIP 8 and 9. How would that be handled?
- CIP 8 with 4 Requirements and 4 tables would become 1 requirement and 1 table. Or use a group heading..
- We will need a new number strategy for interpretations.
- Need the SDT to determine what are the topics. Starting with 9 proposed by the Governance sub-team.
- Rolling each into a requirement. Reporting potential violation. Physical security violations (minor and major). Not sure this is the right way to go.
- There is precedent for lots of standards.
- Helps with granularity. We need to think about all implications.
- List of stuff that needs to be done will be the same. The granularity of the standards will be different.
- Need different frames of references- think about this overnight.
- Its important that the SDT makes sure we have the buckets right. Make sure they are chunked the right way. How it is organized will make a lot of differences.
- SDT should flesh out proposal among the Team. We need to agree on chunking. Get together and decide uniformly and collectively.
- This is a hard subject to get one's head around. Anything changes in format will be initially received as not necessarily simpler. Awareness and staff capacity is an issue in the industry. Practically consider starting what we have.
- Should there be a motion to stay with current CIP framework?
- WECC auditors have indicated that this would be easier with one caveat that tables would need to be numbered. Need a way to track that to the table.
- This does not represent a radical change. In fact, the H/M/L categorization is the radical change. Tables right now don't work. Need to find a way to present appropriately. This is about presentation of requirements.
- About 140 requirements in a single standard. Will violations of any requirement be a violation of standard? This raises repeat violations. Measures more complex and VSLs VRFs.

- Do we have the time to do it? Most of the other teams have requirements written. Significant re-writing will need to be done. Content of both the tables and requirements.
- This will be seen as a radical change in the industry.
- Could improve reporting. Violation of categories. Better reporting overall. E.g. personnel risk assessment. Create a better taxonomy.
- This is the appropriate time to propose the change and get it in front of the industry.
- Changes to software. It will get updated.
- Not lots of additional work. You take requirements. Put together in 1 document. Not a step back in reworking a lot of things. Most requirements are already in a table format.
- This could go faster for us and present a better governance model. Not making changes for no reason.
- What is there to debate if we stick with the current?
- This model is a vast improvement to what we have now. Might be well received by the industry. This team shouldn't concern itself about the vendors. Rather debate the merits of the ideas.
- This approach could help us in terms of consistency checking. Consistency is important. Advantages. Lots of organizational and process changes in the industry. Vendor software is the least of it. If not restating things in multiple places.
- Initially I like it. We have forever been defending one family of standards and we have viewed as 1 standard. We keep as one standard anyway.
- Messy now. Access control and monitoring asset. 5 line requirement. Makes a mess today to figure out what kind of asset is that.
- Many trade organizations are together. NERC CIP, Smart Grid standards coming out. Tracking on 800-53 model. Several doing efforts internally to map all requirements to such a model.
- Granularity for compliance- removing.
- Explained the proposed formats.- 9 topical areas. Policy
- One of the issues- compliance implications of doing that. Now between 8 and 150 requirements. Fewer # and granularity. Single VRF factor. Single V Severity levels . What would they do in terms of an investigation. How report to regions. Penalty calculation.
- Now with 41 requirements moving down to smaller number or having 150 requirements in single standard.
- Putting all standards into 1 document and consist of requirements and table.
- Consider all existing standards 3 -9 into one standard. Requirements have table associated with it.
- As auditors- take requirements and put into table format. Still looking at R and compliance with R. Having worked with military docs. Once you have anything that large and point back in terms of compliance. First time you updated. Move anything else up. From version to version.
- Keeping up to date or compliance tool- hassle in terms of bookkeeping and paperwork accurate.

- R language would be fairly vanilla- table could change. Have policy and procedures with the details.
- 2 action items. Categories need to be finalized and agreed to. Coalesce to action quicker.
- Tom Hoffsetter offered comments

Wednesday evening the Chair asked Howard Gugel to prepare a sample "proof of concept" for the access control requirements to inform a decision regarding format.

D. Review of the Sub-Team Products

Thursday afternoon the SDT reviewed each of the sub-team's draft requirements as revised and refined in the sub-team meetings on Wednesday, offering guidance on various issues raised by the draft requirements.

III. CIP FORMAT REVIEW

A. Tables in the Standard(s)

Howard Gugel, NERC, reviewed the changes regarding format, tables- (R3 referring to table 1). Editing tables. Propose for title to Table R __ helping to tie back.

SDT Comments

- Multiple Rs referring to the same table?
- Keep each table specific with each requirement.
- Bring back question of multiple references to the same table.
- CIP 6- one table and the column as the Rs. Different from the others.
- Need to be consistent for the format for all requirements. Use same format for other tables.
- Consider the guidance documents.
- Rows in table play role of bullet items under each requirement. Separate table links back to each requirement. Resolves issue of multiple rows references back to multiple requirements.
- Grouping the Tables at the end of the standard. Disjointed in a standard. Lot more readable and manageable. Sub requirements, as table entries.
- Similar to attachments in CIP 002. Idea of tables at end, keep requirements concise. Will pose to Maureen to get her opinion. Consistency better at the end.
- Look at Rs and make sure wording is consistent with other requirements.
- Looking at each R how you would measure it. Proof of that- light on this.
- Look at objective statements- read and make sense it is the purpose of the standards.

B. Objective Statements

SDT Comments

- Putting the objective within the requirement? Fraught with danger down the road.
- Enhancing reliability purpose clear.
- Reason it is there, who it applies to why needs to be done.
- Putting in requirement language- gets in the way. Defer that language until requirement language drafted.
- Get requirements first then measures.
- Defer the objectives as part of the requirement. Corollary document.
- If doesn't have a basis in reliability, shouldn't be a requirement.
- Format- R words. Designate.
- The objectives makes it harder to read.
- However it is important to have objective in there.
- Need to be specific about the benefits.
- For now, just bracket the objective.
- Part of the deliverable- measures, VSLs and requirements formats at the end of the session.
- Benefits for reliability? NERC could throw their proposal on each of them.
- Important to deal with measures- know when the requirement been met with. Tangible proof of requirement.

C. CIP Proof of Concept for Format- Access Control

1. Access Control and Auditing- Review for Format

Sharon Edwards presented the work to date on access control including 004 R4, 005 R2, 008 R5 and dispersed throughout the standard.

R1. Account Specifications (007 R 5) **Table**

- Beginning of table- policy should include the following: 20 points. Technical high level controls- H. M. at low- need to understand what they have. #15 "immediate revocation" of access. FERC expectations and SDT's belief of a reasonable starting point. The Sub-team had hard time with this.

Electronic Access Controls

- Sharon noted that this may be redundant.
- Box- "remote access"- Could develop a definition to the standard at hand.

Table R2- Electronic Access Controls

SDT Comments

- Need to decide which formatting for H/M/L.
- Outlier- information protection- document management.
- Measures as previously written- "make available documentation….."
- Haven't tackled VSLs and clean up work. Need sub-team time today.

- Split tables up into more tables? Is violation of one piece, violation of the whole requirement?
- Chunked up more? Good question for further discussion of the sub-team
- Tables provide an improvement and clarity- Keep concept of table. Share concern about multiple violation. Groupings of similar rows and make a separate requirement.
- E.g. Password- under own requirement. Reduces impact re multiple violations.
- Lot of value of tables but reduce the impact in terms of compliance.
- Break into more logical groups and individual requirements.
- Table not to consolidate all requirements. Table facilitates the breakdown of requirement points.
- Table looks good. Clarification. Separate document for audit and monitoring?
- Looked and most of audits related to things NERC would be doing. Didn't develop another table for auditing requirements.
- Row 13- Ports and Services- overlap with Change Management and Operations Security? Probably needs coordination.
- Doesn't specify the content of use restrictions? Is this an issue.
- Wireless approach- didn't want a comprehensive set of wireless standards. Other standards already done a good job. Trying to be less proscriptive. Down the road with encryption. We are not resourced to do.
- What does a blank in the table mean? Clarify if not required or something else.
- Communications aspect of this? Things that are not connected vs. routably connected. Did you intend to stay away from this?
- We did talk about this in the Sub-Team. Spent a lot of time discussing FERC directive to remove access. FERC didn't suggest anything to treat differently. Didn't go down road- may be others. Made decision.
- If talking about remote access, not remote access for user sessions outside of the USPN.
- Format: Required vs. analogue values in the rows. Larger number of individual similar requirements as long as each is a discreet, well worded.
- Breaking out. Barrier. Not having VSL correlated with requirements. Break up or chunk the topic areas – access control.
- When doing measures, have a table form? Matching those in requirement?
- Sub-Team used the generic measures.
- Let's make sure that the SDT knows the topics. E.g. "Security management controls"?
- Repeated wording. E.g. 11 "is required"
- We need a section where you address FERC directives. They had one directive (immediate) Make sure that we cover that for each of the sub-team. We don't need this posting.
- Authentication of un-manned devices. We will see more and more. Will this be covered someplace else? Should this be "human" access control. Do we need to say that?

D. CIP Format Review

1. Overview of Format Questions

On Thursday morning, Howard Gugel presented to the SDT a proof of concept for the access control requirements. He asked the SDT to look at format not merits of requirements in order to get a picture of how the requirements would be presented. He noted the table would be embedded in text and at the end of each requirement. NERC standards review staff agreed with this format approach. This would be the same regardless of which approach is chosen.

- **Option 1.** Keep 003-009 and work from there.
- **Option 2**: retire existing CIP standards and organized by the topics in sequence from 010 on. Access Control e.g. CIP 017.
- **Option 3:** One standards document with 2 sections 010 (002) and 011 (003-009). All controls together. R1 security policies addressing all topics
  - R2 implement per table
  - R3- table for access control
  - R4 implement 2nd table (account specifications).

Initial SDT Member Comments on Format

- Will 002 be on its own? Yes speaking of 003-009 together.
- Where are we capturing connectivity? 005.
- Connectivity is more important than big iron.
- 1st 5 LMH.
- Left column- allows item tracking
- Title Access Controls.
- It will not hard to make change if industry doesn't like this format,
- Language of the table can address connectivity.
- Industry confusion currently in terms of audits at the requirement level. Radical format change may not be well advised.
- Missing opportunity- keep simpler to scope out key things, like was discussed in Austin.
- Tables concept came out of the Phoenix meeting.
- Will FERC have a problem with the tables? There may be no process for reporting on that currently. Process will need to be addressed in this document.
- Common PCI and HIPPA common auditing format for standards.
- Read tables- allows flexibility of the columns. Reporting issue not an issue. Row number tracking will help.
- Table structure agreed to a couple meetings back. We are using them. Whether we keep groupings separate or have a single standard for this is the question. Culture of compliance- repeated violation of standards might be held against the industry with the single format.
- Will it be possible to write a VSL for this table format?

- Separate tables for requirements? E.g. account info and another with remote access issue. Past VSL at requirement level and where with sub requirements. This could end up with a lot of "ors"
- Break out the VSLs with the sub requirements in the table?
- Everything happens at the requirements.
- "Foolish consistency is the hobgoblin of small minds."
- When file with FERC it becomes law.
- Same issue with the VSLs- regardless of options.
- Can split the tables into more areas- can get as granular as the SDT wants.
- Put Rs on left column. Lose the R4 and number Rs. Use if /then construction.
- Now would be the time to propose this. Timing for this.
- Clarification on status quo. Decide on the buckets? We don't do buckets. Stay with 003-009.
- Do some reorganization what is in each standard and possible move- but keep in. Fix for Order 706.
- 003-009 numbering. Moving some Rs around. Tweaking re 706.
- The Team needs to make sure this works. Sees value in topical groupings but has concern with industry confusion. When CIP version 2 was put out the numbering changed and industry members asked why.
- Have a comment form question to get feedback. Makes sense from various standpoints. Ask how much confusion this cause confusion. In the comment form.
- Is there precedent in other reliability standards- if you are generator operator, if you have X, then.
- Limited. Lots based on functional model. Rs directed to different functional entities.
- What ever we do there are going to be changes in the industry. Better we do on our guidance, the better the industry will know what's going on. Need a strong foot forward on guidance.
- Option one- access control. Are they outliers. Easy to place those in a standard.
- Public Comment: Owner operator. Option 3 will be confusing. Is it the whole standard you must follow? CIP have 3-9. Too many changes together for industry to handle. Do option 1.
- Not proposing 4 options. Need to understand difference between 1 and 2 & 3. 2 and 3 carry new organizations. Current standards are supposed to be considered together. They are 1 standard. Change 1 must change all. They are buried and possibly scattered around in the current. New organization with different topical naming.
- Lot of thinking into organization of current standards. Big change is a new organization scheme
- Use tables with all of these options.
- Version 1, 2, 3 confusion- application. Version 4. Renumber standards. Option 2 less confusing.
- Radical change in the standard is required. Some equivalency 3-9 but the approach we are taking and the different formats. Would cause more confusion to use the same numbers. Start for new set 10- onward. Not to be confused with 3-9. Option 2 doesn't follow. It is a

different set of controls organized differently. Likes smaller groupings regarding compliance.

- Tom Hoffstetter noted that he doesn't speak for NERC but that organization in tables is good and he likes the break-out in terms of topics. Required columns will make it a lot clearer for both entity and auditor.
- If we go to option 3- collapse into 1 standards. 140 controls in one standard. Violation more than1 get a penalty.
- Whole different paradigm require a new approach as to how penalties assess. Approach different in many ways. Wouldn't try to make current structure fit. Have to depart from traditional approach to penalties. Have to describe them differently and assess in a different format. Across the board.
- Nothing to argue with what TH said. These standards will be balloted and posted and implemented under the current process.
- Option 3 recognizes how tightly knit these are together.
- This may not matter in the end. Push in his company.
- Can NERC help with this issue that RK brought up? What is the audit standpoint. Can they do this. Might help to present options 2 and 3 at the Technical Workshop. Show how NERC and auditors of regional areas would handle. How models would be handled in audit and penalties.
- Option 3- organization within? Still the same? Structured as per 1 or 2?
- Constrained by current compliance structure. Could we propose a new approach? Put out standards with a proposed structure?
- Confined now to VSR VSL structure.

2. Initial Preference Ranking of Options and Voting for the Preferred Format Option

The Team following the discussion of the pros/cons of the options, voted first on each of the three options indicating its acceptability. Following that each Team member voted to support the option they found most acceptable or preferable based on the discussion and their perspective.

Format Option 1: keep existing CIP 003 to 009 in its current form maintaining its existing logical construct (may involve minor movement of existing requirements between standards)

Yes	*No*	*Indifferent/could go either way*
8	**7**	**3**

Format Option 2: Retire 003 to 009, create new CIP 010-16 grouping according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**2**	**6**

Format Option 3: Collapse CIP 003-009 into a single standard that contains all requirements created/edits by small groups and grouped according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**7**	**2**

The team then voted for one of the two highest ranked options under consideration:

- Option 2: Retire 003 to 009, create new CIP 010-16 grouping according to small group assignments. ***Yes*=6**
- Option 3 Collapse CIP 003-009 into a single standard that contains all requirements created/edits by small groups and grouped according to small group assignments. ***Yes*=10**
- *Abstained from voting for Option #2 or #3:* 4

Comments on the Options Ranking and Next Steps for the Sub-Teams

- Need to take into account the industry's reactions.
- Don't see any real difference between option 2 and 3.
- Not a single requirement vs. standard.
- It is different in terms of what is presented. Violation of any requirements may present problems.
- This is just an organization issue.
- What are the expectations for Sub-teams in terms of drafting VSLs?
- Allowed to have content- for each row of your table a VSL statement in that format.
- Finish up writing requirements. We can pull back together into multiple standards or into one standards following a decision.
- Would be helpful to go through one of the sub-team's reports before breaking. Substance requirements, measures and VSLs.
- Missing several definitions. Should we use boxes? Indicate it is guidance. If not, it will be exported to glossary, or in requirement.
- Note if put in guidance then not part of standard. If it goes out without guidance document. Comments won't be complete.
- As a reality check, take access control and go through it and reframe expectations. Going to need work after going out for informal comment. Interim work product posting. Work as hard. Focus on requirements.
- Some sub-teams are using different definitions for external connectivity. Factor into what is put in the rows on table. Each needs to do the walk through.
- Five remaining areas that need SDT guidance for sub-teams.
  - Square box definitions- specific to standards (vegetation management standard precedent
  - Control centers definition
  - Different types of communications
  - How should the sub-team address drafting measures or consider putting out document for industry review without measures

  - Address VSLs or consider putting out document for industry review without measures
- SDT should clarify outliers- definitions. Whose will be used? When will see all the definitions in the various document?
- Governance section, based on SDT input pulling policy statements up.
- Suggest that a SAR for a drafting team be considered. Address FERC 706 items that may be outside the scope of drafting team, e.g. NIST risk management framework.
- 9 Categories of proposals to organize. Put the level of controls in right hand columns or separate rows.
- Option 1. Allows different time frames. Separate line items for medium. Time frames in columns. Bulleted lists time frames.

3. Reviewing and Ranking Option 2 (2nd Round)

At the end of the day the Team took up the format issue again. The Vice Chair made a proposal that the Team use Option 2 (which would renumber the requirements using the topics to organize them. The Team discussed this option:

- Consider renumbering 002 as 010 – confusing to have 002 then renumber at 010
- Posted previously as 002, proposed keeping then renumbering new.
- Yes, different titles for the same thing that exist with a few split out.
- Some match what we have now, some are new – where we can group into the existing CIP we could do so and renumber only the new ones.
- Is media protection now media disposal? Where would you move information protection?
- How many teams work on multiple standards at the same time? Yes, others teams do address more than one but not ten of them
- The titles may seem the same but many of the sub-parts have been moved around except for 002 which is still focused on the same topic area – we would need to educate the industry on what is in each standard.
- Rename the last item 021 as Boundary protection rather than data communications?
- Will we map old standards into the new ones? If so, why not retain some of the old numbers
- Did not gain consensus on this earlier – this seems ad hoc.
- We probably need to agree on something today in order to to put this into a format.
- Propose altering proposal to start with 010 for old 002 – new numbers for all of them – less confusing
- Access control needs to be separated into physical and electronic.
- Under personnel and training – would that include training for all the other standards?
- Idea is to combine training and awareness and risk assessment.
- Change name of the last one and make electronic access protection or role into new 013 under system security?
- Heartache at pulling physical access control out as separate item.
- May still need further renaming or organization as we move forward.

- We have to write the standards so we are not assuming IT security and physical security will be handled by the same people
- Physical security and access control – IT controls access to server but not the badging for physical security –
- Need to go with this not as a concept but as framework – it is a format

The facilitators polled the team on their support for the option #2 (multiple standards) and 7 of 16 members were in support of utilizing this as the format.

An additional member joined and the Team then tested support for Option 3 (putting all into single standard) and 9 of 17 supported using this format. Neither format approach received sufficient support to make an SDT decision.

4. Numbering the Requirements

The Team them reviewed and tested support for each of the following propositions:

- **Change from existing CIP numbering system?** Yes- 13 favor changing (of 17 = 76%)

SDT Comments

- Adopting the headings would be the same under multiple numbers or as one
- If we keep CIP 002 as 002 for continuity then the rest are renumbered or just one,
- would be more confusing
- change to Option 2 if we revote but concerned this is under duress
- Think we need just one standard

5. Adopting Category Headings for Requirements

- **Adopt the proposed headings for the requirements as the categories whether as one or multiple standards** – Yes-13 (of 17 = 76%)

After further Team discussion it was determined that there was no longer a quorum and the Chair suggested postponing further discussion until Friday morning.

6. Final Review of Format Options

On Friday morning the SDT took up the final review of format options for the informal posting document(s) in order to make a decision.

The facilitator suggested the SDT use an acceptability ranking of the two possible format options that had been discussed and debated yesterday followed by clarification of concerns to see if they could be met and a requisite number of members could agree on the format to use for the informal posting.

He reviewed the scale to be used as: 4= fine as is, 3= support but have questions, 2= need to address concerns before I can support, or 1= cannot support. The SDT then ranked each option and those providing a 2 or 1 offered what their concern was.

Option #2 – Requirements in Multiple Standards

- Use the Topical areas discussed on Thursday and utilize multiple standards (example CIP 010 -020). CIP 002 also gets re-numbered.

4-3 3=7 2-6 1-0 (Avg. 2.81)

Option #2 Concerns

- All the standards have a single purpose and are meant to be viewed as one. Should be one for clarity.
- Efficiency of one (better implementation) - Don't like fragmentation between multiple standards.
- Much cleaner to have just one standard
- Current standards say to consider as one but in fact they are not treated that way thus making compliance difficult.
- There is a greater chance for double jeopardy. Easier to manage with Option 3 in a single standard format. Fragmentation leads to fragmented implementation rather than unified management.
- We do talk about the CIP standards as one but in practice they are treated differently.
- I like the grouping or headings but multiple standards looks like we are asking them to do more - also additional documentation
- If we post additional standards, the reaction of industry will be that we are asking them to do more. Having only one standard will reduce required documentation. Eventually multiple standards would be on different version levels, thus adding to confusion.

Option #3 – Requirements all in One Standard

Use the Topical areas discussed on Thursday, but one new standard is posted containing sections for.

4=6 3=5 2=3 1=2 (Avg. 2.93)

Option #3 Concerns

- Compliance implications - violating one standard even if different requirements- significant increased risk for multiple violations of one standard.
- Need to hear technical argument to support 3
- Compliance issue- non-compliance on low items makes you vulnerable to citations for repeat finding of non-compliance
- Compliance my main concern- tie our hands about splitting later- once merged cannot deal with future revisions separately
- Just trying to format for posting

- Concerned about complexity- more than value of unified
- Voted a 1 because of the number of requirements and sub-requirements. There are about 120 major requirements plus sub requirements. The 140 plus requirements may means that any violation of any of these requirements you are in violation of one standard. Compliance reporting and compliance sanction issue on the issue of multiple violation of the standard.
- When RSAW's are prepared, the SME should only view information pertinent to his area of expertise.
- Agree with concern about repeat violations of the same standard.
- Can the compliance situation could be fixed if the structure of the way NERC viewed the standards for sanctions, etc. were changed? However, that will not change.
- Is it likely that NERC would change the way they viewed compliance to support Option 3?
- Concern with the sheer complexity of the one standard. Also see disadvantages of the lack of a unified approach, but there have also been advantages in the divide and conquer approach.

SDT Options Discussion following the Ranking

- Fragmentation of the standards will contribute to lack of a unified management and implementation.
- Sometimes the only change in a standard is the change in the standard number. This makes no sense. If you look at the categories we approved yesterday, there will be tighter integration between the CIP standards. If we have separate standards, we need to make sure each can stand alone.
- Prefers the unified standard and believes that we can help the complexity by making them one. The big concern is the regulatory impact mentioned by others.
- The Current standards do not lend themselves to good organized implementation. The new adopted topic areas are the most important thing to consider. Can both options be presented to the industry for feedback?
- The facilitator asked NERC staff is we need one or the other for the posting?
- Scott Mix noted that raw work papers will not be sufficient for the posting. Presentation in two formats will likely confuse the industry. Perhaps the posting could be presented in one format, but we explain the other format and ask the industry to comment on whether they like the change or not.
- Scott Mix showed the Team the NERC generated report does show total violations by standard.
- Howard Gugel submitted the enforcement question to Joel DeJesus at NERC concerning compliance concerns. Is there a compounding effect? A: If there are multiple impacts of multiple violations of the same standard, there may be some compounding effect. If R3, R12, and R22 were violated, they would be separate violations with no compounding effect.

- The concern is the "culture of compliance" at NERC and FERC. If the same standard is violated, it will have the consequence of doubting the culture of compliance.
- If we get one single standard that has magnitudes of violations, it will send the wrong message and numbers of violations will be noticed.
- In terms in the ability to observe, Scott Mix suggested he did not see the difference.
- All the reports to the member committees are by standard number and he believes there will be a spike if all CIP is one standard.
- Legislators are aware of the collections of standards that the industry must deal with. For example FISMA is a collection they are familiar with.
- We need a decision. We spent too much time discussing this. We have agreed on the categories. Let's get something out there. We are wasting too much time.
- We could debate this all day, but we need to move forward.
- If we step away from CIP and started talking about vegetation management, he believes breaking the standard into multiple would not make sense.
- Lawmakers and congress will understand and support that while there are multiple topics, there is still one framework for improving cyber security implementation.
- Do we need a transition before moving dramatically to either new set?
- These categories make it hard to divide responsibility.
- Think new categories provide better organization and will improve implementation.
- Can we put out both as two separate documents?
- That may be too confusing to address option with questions in comment form
- Need to be accountable.
- We need to put a question to the NERC enforcement side. Can we go with this and limit compounding violations?
- Concerned about potential impact on Congress if there is a spike in non-compliance because multiple violations of one standard.
- Congress is most concerned about fragmentation and used to looking at one standard for an industry.
- The facilitator asked if any concerns addressed that would move their vote from a 3 or 4?
- Some members expressed concerns about suspending rules- changing the game. Needs to be a yes/no choice
- Concerned adding in "either" result in super majority for both options - then what?
- Is there an alternative embedded in the decision rules for this post for informal comment? Can the SDT use a majority (50%+) for purpose of posting using single standard or multiple standards and documenting the SDT differences in comment form for either choice.

The 17 SDT members present then voted for their preference for posting for informal comment between the two options with the following result:

Option #2 (multiple standards) **Yes = 6 (35%)**

Option #3 (single standard) **Yes = 11 (65%)**

The SDT agreed that while this decision to post for informal comment has a majority support (65%) but not the super majority (75%) of the members called for in the decision rules, the Team is asking for industry comment and input on the formats through comment form before finalizing a format to present in the formal comment draft in July, 2010. The Team discussed that this approach is consistent with the spirit of the following consensus rule provision: "In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team."

IV. NEXT STEPS AND ASSIGNMENTS

On Friday the Chair reviewed the schedule, assignments and next steps for the SDT to produce a final version for posting on May 3, 2010. Joe Bucciero will lead with assistance from Howard Gugel the drafting of comment form with information provided by each of the team leads and will also add a question from discussion of the format to document discussion

The SDT will need to begin creating an implementation plan for posting in July for formal comment with a small group of SDT members in order to provide some frame for discussion at the May meeting and to answer any questions at the May workshop in Dallas. Scott Mix will be looking for individuals to work with – this will occur after May 3.

We need something in cover letter for May 3 posting that speaks to the SDT's philosophy on implementing the plan – industry needs to understand what we are doing. Need a couple paragraphs explaining our approach or intent Jackie Collett, John Lim and Doug Johnson agreed to work with Scott Mix on developing a draft implementation plan.

The Chair reviewed the schedule from April 19, Monday to posting on May 3, Monday. It was agreed the sub-teams need to complete their drafting and get these to Howard to put into "standard" for review by NERC staff. The plan will be to assimilate the NERC comments with team leads, then late in last week of April have a ready-talk and email vote for approval to post on May 3. Have conference call on April 26 for team leads and 29th for ready-talk review with full team Each Sub-team lead will seek to get work done and to Howard Gugel by Monday morning then review with Howard and team leads on Tuesday afternoon. The following schedule was reviewed and approved by the SDT:

- 19th by 5:00 – requirements, measures, vsl's and glossary drafts to Howard
- 20th Sub-team leads with Howard at 3:00 – 6:00 EST

- 21st Howard will get team drafts to NERC staff for review
- 27th full day (10-5) meeting with NERC staff with Sub-team leads and anyone else who wants to join (NERC comments back by 26th if possible to full team – concern is legal and compliance) – updated version send out on 28th to full team for review
- 29th full team meeting (1 to 4) for review and vote to post

The Chair and Vice Chair and the SDT thanked Jay Cribb for his excellent hosting and great facilities.
The meeting adjourned at 12:00 p.m.

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 20th Meeting Agenda
April 13, 2010, Tuesday- 1 PM to 5:30 PM EST
April 14, 2010 Wednesday- 8 AM to 6:15 PM EST
April 15, 2010 Thursday- 8 AM to 5 PM EST
April 16, 2010 Friday- 8 AM to 12 PM EST
Georgia Power
241 Ralph McGill Blvd
Atlanta, GA 30308
NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the revised CSO 706 SDT 2010 Work plan and Schedule
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and the May 2010 Technical Workshop
- Review, refine and adopt the Draft Final CIP-002-4 for industry informal comment
- Review, refine and adopt the Sub-Team Security Control Requirements draft for industry informal comment
- Develop related CIP 002 and Security Controls Requirements Guidance Documents
- Agree on next steps and assignments

Draft Agenda

Tuesday **April 13, 2009**
1:00 p.m. Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair*

	Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of March 9-12, 2010 Phoenix SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review and Discussion of CSO 706 SDT Workplan and Schedule - March-December, 2010- *Stu Langton*
1:45	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:55	Update on CIP Communication Plan and May 2010 Technical Workshop - *Carl Dombek*
2:15	Overview of Single Text- CIP-002-4 & Security Controls Requirements
2:45	*Break*
3:00	Review of Revised CIP-002-4 Draft Final and SDT Industry Response Document- *CIP-002-4 Drafting Team, John Lim et al.*
3:30	Full Team Consensus Testing on Refinements of draft final CIP 002-4
5:25	Review of Proposal for Wednesday Agenda
5:30	*Recess* ▪ *Possible Security Controls Requirements Sub Team Meetings- Evening* ▪ *If needed, CIP-002 Drafting Team to meet to finalize draft and present for adoption Wednesday morning.*

Wednesday	**April 14, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Final Review of CIP-002-4 as revised
9:00	Security Governance Requirements- Overview and Consensus Testing
10:30	Break
10:45	Personnel and Physical Security Requirements and Guidance- Overview and Consensus Testing
12:15	Working Lunch
1:00	Operations Security Requirements and Guidance - Overview and Consensus Testing
2:30	Break
2:45	Recovery and Response Requirements- Overview and Consensus Testing
3:45	Access Control and Auditing- Requirements- Overview and Consensus Testing
5:00	Change Management, System Lifecycle and Information Management- Requirements- Overview and Consensus Testing
6:15	*Recess* ▪ *Possible Security Controls Requirements Sub Team Meetings- Evening*

Thursday	**April 15, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Security Controls Sub-Teams Refinement Sessions
10:00	Break
10:15	Security Controls Sub-Teams Refinement Sessions
12:00	*Working Lunch*

1:00	Full Team Review and Consensus Testing on Final Draft
3:00	Break
3:15	Full Team Consensus Testing on Refinements-*Continued*
4:15	Motion to Adopt in Concept Draft CIP 002 and Security Controls Requirements for Informal Comment Posting Review Any Drafting Assignments and Friday Agenda
5:00	*Recess* ▪ *As needed ad-hoc drafting groups- Evening*

Friday	**April 16, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Sub-Team Development of Guidance Documents
10:15	*Break*
10:30	SDT Review and Suggested Refinement of CIP Guidance Documents
11:15	Review of May 2010 Technical Workshop Planning and Preparation
11:45	Review of Dallas Agenda and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

Appendix # 2 Attendees List
March 9-12, 2010, Phoenix, Arizona

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT (T/W/Th)
3. Jay S. Cribb	Southern Company Services
4. Sharon Edwards	Duke Energy
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Gerald S. Freese	America Electric Pwr. (T/W/Th)
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Frank Kim	Hydro One Networks Inc. (T/W/Th)
10. Rich Kinas	Orlando Utilities Commission (Th/F)
12. John Lim, Chair	Consolidated Edison Co. NY
13. David Norton	Entergy (T/W/Th)
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy (T/W/Th)
16. Jonathan Stanford	Bonneville Power Administration
17.Tom Stevenson	Constellation
18.Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
19. John Van Boxtel	WECC
20. John D. Varnell	Technology Director, Tenaska Power Services Co.
21. William Winters	Arizona Public Service, Inc.
Scott Mix	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center
Tom Hoffstetter	NERC (Thurs a.m. by phone)

SDT Members Attending via ReadyTalk and Phone

22. Jackie Collett	Manitoba Hydro
23. Patricio Leon	Southern California Edison (T/W/Th)
24. Kevin Sherlin	Sacramento Municipal Utility District (Th)

SDT Members Not Participating

Joe Doetzl	Kansas City Pwr. & Light Co

Others Attending in Person

Jim Fletcher	AEP
Brian Newell	AEP
Bryn Wilson	OGE
Clyde Poole	TDITX
Rod Hardiman	Southern Company
Elizabeth Moses	Georgia Transmission
Jason Marshall	Midwest ISO

Others Attending via WebEx and Phone

Andres	Lopez	andres.lopez@usace.army.com
Justin	Kelly	FERC
John	Fridye	jfridye@rrienergy.com
Steve	Newman	srnewman@midamerican.com
Maggy	Powell	margaret.powell@constellation.com
Bill	Keagle	william.a.keagle.jr@constellation.com
Steve	Newman	srnewman@midamerican.com
Jerome	Farquharson	jfarquharson@burnsmcd.com

Appendix # 3 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that
violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect
NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Sub-groups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.

- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Sub-groups) may have a negative impact on particular entities and thus in that sense adversely
impact competition. Decisions and actions by NERC (including its committees and Sub-groups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Sub-group, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on

- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
APRIL –DECEMBER 2010

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting-Atlanta, (4/13-16)	4/12/2010	**Present Controls draft for full team review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
	4/19/2010	**NERC Prepares Full Package for Industry Comment**
	4/26/2010	**SDT Reviews and Approved Full Package for 30-day Industry Comment Period**
5/3/2010	5/3/2010	***Informal Comment Posting for full package starts Completes on 6/2/2010***
SDT Meeting-Dallas, (5/11-14)	5/10/2010	**Prepare for Industry Workshop**
5/19 & 5/20/2010	5/17/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
	5/24/2010	**SDT Considers Comments from Workshop**
6/4/2010	*5/31/2010*	***2nd Informal comment period ends***
6/2/2010		***Comment Period Ends***
6/3-6/4/2010		***SDT Summarizes Comments Received***
SDT Meeting, Sacramento (6/8-11)	6/7/2010	**SDT Meeting: Comment review, response process, re-drafting, as needed**
	6/14/2010	Sub team meetings
	6/21/2010	Sub team meetings
6/29/2010	6/28/2010	Sub team meetings. SDT interim online meeting.
	7/5/2010	Subteams Package modifications into Standard documents
SDT Meeting, Pittsburgh, (7/13-16)	7/12/2010	**Finalize & Approve Documents for posting for 45 day formal comment period**

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
	7/19/2010	***NERC Prepares Materials/SDT Approves Revisions/NERC Seeks SC Approval for Ballot***
7/26/2010	7/26/2010	***45 Day formal comment period starts (completes 9/8/10) /Ballot Pool formation (completes 8/25/10)***
	8/2/2010	**Industry Comments on Standards**
SDT Meeting, TBD, (8/10-13)	8/9/2010	**SDT Meeting: Prepare for Industry Webinar**
8/18/10	*8/16/2010*	***Hold Industry Webinar***
8/25/2010	8/23/2010	***30 Ballot Preview/Initial Comment Preview ends/Ballot Pool formed***
8/30/2010	*8/30/2010*	***Initial Ballot Starts***
SDT Meeting Winnipeg, (9/7-10)	9/6/2010	**Respond to comments received. Drafting revisions. Review Ballot Results and Additional Comments**
	9/8/2010	**Initial Ballot Ends**
	9/13/2010	Sub team meetings
9/24/10	9/20/2010	Sub team meetings; Full SDT on-line meeting to adopt revised draft of documents
	9/27/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
10/4 to 10/13/10	10/4/2010	Re-Ballot Period Begins
SDT Meeting TBD, (10/12-15)	10/11/2010	**Prepare responses to 2nd ballot comments**
10/19/2010	*10/18/2010*	***Sub-teams meet to adjust requirements***
10/29/2010	10/25/2010	***Prepare & Finalize revisions to standards and responses to comments on standards***
	11/1/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
11/8 to 11/17/2010	11/8/2010	3rd Ballot Period Begins

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting TBD, (11/16-19)	11/15/2010	**Prepare responses to 3rd Ballot comments**
	11/22/2010	*NERC & SDT finalize responses to ballot package*
	11/29/2010	*Seek SC & BOT Approval for Filing*
	12/6/2010	*Seek SC & BOT Approval for Filing*
SDT Meeting TBD, (12/13-17)	12/13/2010	**SDT Meeting to review Filing and Celebrate Project Completion**
	12/24/2010	*Submit for Regulatory Approval*

Appendix #5

CSO 706 SDT DRAFTING SUB-TEAMS

Sub-Team	NERC Standards and DHS Control Families	Team Members
Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton
CIP 002-4	Draft revisions to CIP-002-4, and Summary of Responses to Industry comments	John Lim, Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton *Rod Hardiman (Observer)*
Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell
Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*
Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Mainten. DHS 2.9 Information and Document Mgt. DHS 2.13 Media Protection	Keith Stouffer, Phil Huff (Lead) *Observer Participants: John Fridye*

Security Controls Sub-Team Principles and Drafting Guidance

CSO 706 SDT SECURITY CONTROLS SUB-TEAM DRAFTING PRINCIPLES

(ADOPTED BY CSO 706 SDT, JANUARY, 2010)

1. Applicability [NERC ROP] Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted.	**9.Practicality** [NERC ROP] – Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
2.Reliabiliy Objective [NERC ROP] Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system.	**10. Consistent Terminology** [NERC ROP] To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.
3.Performance Requirement or Outcome (NERC ROP) Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest.	**11. Commensurate Controls for BES Impact Categories.** Security controls shall be commensurate with the identified level of BES impact categories.
4. Measurability (ROP) Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement.	**12. Change Documentation.** Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes: a. Above and beyond the current standards; b. Removal of requirements; and c. Major formatting changes.
5.Technical Basis in Engineering and Operations [NERC ROP] Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.	**13. Reduce Administrative Overhead**. Administrative documentation shall be kept to the minimum that is necessary
6. Completeness (NERC ROP) Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.	**14. Priority.** Implementation plans for the Standards are prioritized according to level of BES impact.
7. Consequences for Non-Compliance [NERC ROP] In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.	**15. Eliminate or Minimize TFEs.** Security controls shall eliminate or at least minimize the need for TFEs. Allow for compensating controls to mitigate the need for a TFE.
8. Clear Language [NERC ROP] – Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.	

SECURITY CONTROLS SUB-TEAM
PROCESS AND DRAFTING GUIDANCE AND DELIVERABLES

Guidance from the January, 2010 Tucker Meeting and the February 2010 Austin Meeting

For the purpose of maintaining consistency across the teams and capturing interim decisions and change documentation, each team should utilize the following development process:

1. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
2. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
3. **Specific not Prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
4. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
5. **Develop the requirement language** for each security control identified in step 1.
   a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
   b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog*.
6. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
7. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
8. **Address specific directives from FERC Order 706** that may be applicable to the requirement.
9. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, consider the cost in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
10. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
11. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.

(c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.

12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.