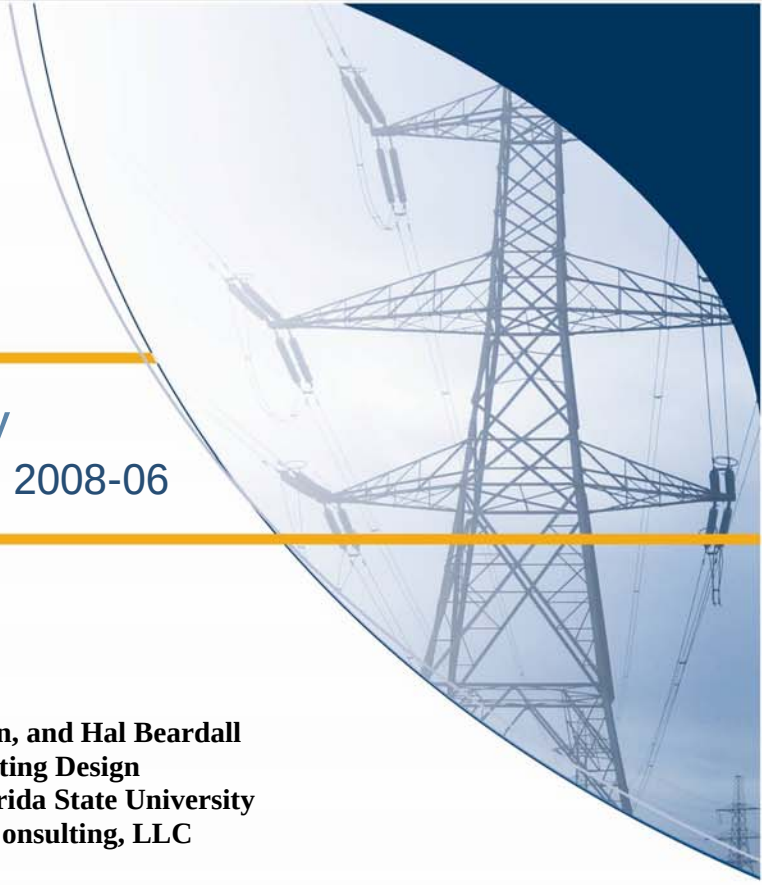
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



16th Meeting Executive Summary

Cyber Security Order 706 SDT — Project 2008-06

December 15, 2009 | 8 a.m. to 5 p.m. EST
December 16, 2009 | 8 a.m. to 5 p.m. EST

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary Contents

EXECUTIVE SUMMARY

On Wednesday morning, the Chair welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. After the Chair reviewed the meeting objectives, Mr. Bucciero reviewed with members the need to comply with NERC's Antitrust Guidelines. On Thursday morning, the SDT approved, without objection, the meeting summary for the November meeting in Orlando. Following lunch on Thursday, the SDT congratulated and applauded Jeri Domingo Brewer on her leadership role in chairing the team for the past 15 months and Phil Huff and John Lim presented her a plaque on behalf of the SDT in recognition of her leadership by example.

Gerry Adamski, NERC Director of Standards, reviewed with the team the NERC efforts to provide support for the team as they confront the challenge of completing the CIP in 2010. He offered that the new President of NERC has indicated that this is one of its most critical projects in the coming year.

He recounted that NERC had projected a two-year time frame for the project which will be realized if the SDT can complete its work by December 2010. He suggested that the SDT must demonstrate that CIP 002 Version 4 and the controls in CIP 003-009 will improve the current critical asset identification process and this has both technical requirements and political overtones.

Since the SDT November meeting in Orlando, NERC has identified a critical path to accomplish two things: a quality CIP 002-4 revision by June 2010 and the related set of security controls/requirements by the end of 2010. NERC has been working on how to put an optimal framework in place to allow the delivery on the expectations for the SDT. He noted a couple offline meetings with industry leaders and the SDT leadership have led to identifying NERC actions that can assist the Team. NERC met with trade associations collectively on November 30, 2009 to solicit their support and to build a mutual understanding of the technical and political complexity involved in the updating the CIP. In support of the SDT's meeting process, NERC has committed to implementing a comprehensive communication campaign and has secured additional support with Roger Lampila from Compliance and Dave Taylor and Howard Gugel from NERC Standards, in addition to Scott Mix's expertise, and introduced Lauren Koller from NERC who will assist and help Joe Bucciero on the ready talk and document displays. He noted that the Standards Committee met earlier in December and approved the use of an informal comment period followed by a formal 45-day comment period. He asked the Team to continue to help NERC understand what is needed to get the job done.

The Chair welcomed and introduced Barry Lawson with the National Rural Electric Cooperative Association (NRECA) and current chair of NERC's Critical Infrastructure Protection Committee (CIPC) and Allen Mosher representing the American Public Power Association (APPA) and vice chair of the NERC Standards Committee**.** They reviewed the letter sent to the Team by five trade associations including NRECA, the Edison Electric Institute, the American Public Power Association, the Electric Consumers Resource Council and the Electric Power Supply Association. They offered to provide any support that the trade association could in support of the industry's self regulatory model and industry developed standards. They asked the SDT to let them know what they can do to help. The Trade Associations agreed that:

- The Industry must seek to eliminate subjectivity as much as possible from both a technical and political standpoint.
- The SDT should identify the "brightest lines you can come up with".
- Trade associations are not suggesting how to do this. The current draft has made huge steps in the right direction.

- If we don't get the CIP standards right there will be real consequences for the Industry including a potentially reduced role in the development of these standards.
- The SDT's framework for the CIP appears sound and makes intuitive sense. Develop an asset classification approach that will make sense to the industry.
- The trade associations pledge to try to get our respective members to give early, responsive and constructive comments to the SDT on its drafts.

On behalf of the SDT, the chair noted appreciation for the work and efforts of NERC and the Trade Associations in assisting the SDT in its efforts to draw up a new CIP.

John Lim then provided an overview of the work undertaken and the changes made to the CIP 002-4 draft documents between Orlando and Little Rock by a drafting group comprised of John Lim, Jackie Collett, Phil Huff and John Varnell. These included the CIP 002, the Guidance Document, the Introduction and Comment Form and the Control examples. Dave Taylor noted that Howard Gugel from NERC will help the SDT get next products up to speed and be able to work with the SDT to answer any questions regarding format.

Jackie Collett provided an overview of the Pinecone Power "walk through" exercise. The SDT broke into two small groups and engaged in a "walk through" exercise. Following the break outs, the SDT reviewed reflections on lessons learned from the walk through in terms of implications for improving or clarifying the CIP 002 draft, including:

- Clarify how to define BES sub system in requirements and/or guidance
- Determine Appendix 2 requirement in standard
- Clarify blackstart units that change: How to address this in requirements? "blackstart capable"
- In terms of generating subsystems — define "Plant" — Units, combinations.
- R1 — "Identify + Categorize"? vs. Categorize.
- Keep cyber for R3? Not in R1 — rely on applying criteria.
- How to address "combinations" in the subsystems? Start with cyber systems first?
- Appendix #2 "Must Identify" a requirement with appendix.
- Careful we do not oversimplify categorization which may result in over protection — too many shortcuts could lead to incorrect conclusions.
- Need a full assessment without requiring more work than is necessary.
- We want to be sure nothing is missed — doesn't matter how it is defined if it is covered — then can choose to make it a subsystem but are not required to
- Give entities flexibility but careful don't leave an opportunity to game system by breaking systems into parts that stay below threshold for "high"
- Clarify something in R3 — identify and categorize all BES subsystems ….. that means identify every part of cyber system that has anything to do with awareness function — is that what we meant?

Following the Walk Through, the SDT reviewed the remaining issues and agreed to work in the following Drafting Groups on Wednesday afternoon to address issues raised in the "Walk-Through" and bring back clarifications and refinements for consideration by the SDT.

- Group #1 addressed Requirement #1and reviewed and produced agreement on how to address the R1 and appendix issues that had been raised in the walk through.
- Group #2 addressed Requirements #3 reviewed and produced agreement on how to address the R3 and appendix issues that had been raised in the walk through.

At the end of the day, the SDT reviewed progress and noted the following assignments:

- Issues of reliability functions— Phil Huff noted a plan to meet for dinner and resolve these issues and bring suggestions back tomorrow first thing tomorrow.
- Break into groups for document drafting (introduction and comment form; CIP 002-4; Guidance Document; Appendices; and Sample Controls.

Chair reminded the SDT that the goal is to ensure posting for informal industry review and the SDT should expect many suggestions back from industry. She also checked with the SDT to see if there were any red flags on proposed list of FERC specific directives in 706 since it will be part of the NERC filing at the end of December. The SDT concurred with the list.

On the second day John Lim reviewed with the SDT the revised definitions of terms used in standard and the SDT thoroughly discussed and reached consensus on issues in the definitions section.

Phil Huff led the SDT through a discussion of the changes to the standards sections R1, R2, R3 and R4. The SDT polled support for a couple of propositions including:

- **R-1. —** TPO requirements call for "annual" evaluation. SDT Poll support for reinstating the term "annual" in the standard for CIP-002-4 draft for industry comment: Yes — 8, No — 10. Won't reinstate "annual" for CIP 002-4 draft.
- **R4**.— Is the senior manager the right one for this role? If not, then does this requirement do much? The members ranked acceptability of the following options (multiple votes were permitted):
  - Remove it, address it elsewhere: 10 votes
  - Keep in R2 but with fuller definition: 9 votes
  - Keep it here as is: 7 votes
  - Remove here and keep in the comment form: 1 vote

  Members then offered the following preference polling *(only one vote for one of the 3 options)*
  - Remove it, address it elsewhere: 8
  - Keep in R2 but with fuller definition: 5
  - Keep it here as is: 1
- There is consensus of the importance of the issue and inclusion of the senior manager but less clear how best to do it.

The SDT then reviewed and refined the Compliance Section, the VSLs section and the Attachment documents.

On Thursday afternoon a motion was made and seconded to approve CIP 002-4 with identified and agreed upon changes. 16 members voted in favor, 0 members opposed and 1 member abstained.

Following a break, the SDT broke into separate "document" groups to harmonize the comment form and guidance document with the adopted CIP 002-4 (e.g. the Introduction and Comment Form and the Guidance Document). At the conclusion of the small group refinements to these documents the SDT reviewed the following key issues for the future (i.e. "parking lot")

- More detail on reliability functions to make operational — address "over protection" issues — map Requirement Function to thresholds
- "Controls" — "secure" defined — address in 003-009
- "BES Subsystem Impacts" define going forward (high/medium/low)
- 1.7, 1.11 & 1.15 — control center function issues)

The SDT Chair and Vice Chairs reviewed with the Team the work plan going forward including the need to make progress on the security controls (CIP 003-009) at the SDT's January meeting in Tucker, Georgia. The chair thanked Phil Huff for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 3:30 p.m. on December 16, 2009.

I. AGENDA REVIEW AND UPDATES

A. Agenda Review

On Tuesday morning, the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On the second day the SDT approved without objection the meeting summary for the November meeting in Orlando.

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.

Following lunch on Thursday, The SDT congratulated and applauded Jeri Domingo Brewer on her leadership role in chairing the Team for the past 15 months and Phil Huff and John Lim presented her a plaque on behalf of the SDT in recognition of her leadership by example. The Chair thanked the members for the acknowledgement and encouraged them to build on their work to date to get the job done by the end of 2010.

B. Review of NERC and Trade Association Actions in Support of CSO 706 SDT

Gerry Adamski, NERC Director of Standards, reviewed with the Team the NERC efforts to provide support for the team. He noted his admiration and appreciation for SDT commitment and dedication to this challenging task and that he believed it was Evident that all members are making a difference. He expressed his hope that the

Team could continue to move forward expeditiously with the task in the coming year. He offered that the new President of NERC has indicated that this is one of its most critical projects in the coming year.

He suggested that the Team will be challenged in addressing and finalizing CIP 002-4 while simultaneously developing CIP 003-009 addressing a significant portion of Order 706 directives. He reported that the Recirculation Ballot for Version 3 received 85.6% approval and that the NERC Board of Trustees was set on December 16 to approve version 3 and send on to FERC.

He recounted the "whirlwind of activities" over the past year and half and the call to action with respect to delivery of critical infrastructure standards. NERC had projected a two year time frame for the project which will be realized if the SDT can complete its work by December 2010. The SDT must demonstrate that CIP 002 Version 4 and the controls in CIP 003-009 will improve the current critical asset identification process and this has both technical requirements and political overtones.

Since the SDT November meeting in Orlando, NERC has identified a critical path to accomplish two things: a quality CIP 002-4 revision by June 2010 and the related set of security controls/requirements by the end of 2010. NERC has been working on how to put an optimal framework in place to allow the delivery on the expectations for the SDT. He noted a couple offline meetings with industry leaders and the SDT leadership have led to identifying NERC actions that can assist the Team. NERC met with trade associations collectively on November 30, 2009 to solicit their support and to build a mutual understanding of the technical and political complexity involved in the updating the CIP.

The Trade Associations are hoping the new CIP will provide clearer delineations in categorizing critical assets, i.e. "more bright line" determinations. The hope for is for producing a standard that is more objective than subjective and that provides an entity the understanding of which category their assets fall into.

In support of the SDT's meeting process, NERC has secured additional support with Roger Lampila from Compliance and Dave Taylor and Howard Gugel from NERC Standards, in addition to Scott Mix's expertise. Mr. Adamski noted that he has collected internal NERC comments on the current CIP 002-4 draft and will provide feedback to the SDT later at this meeting. He also introduced Lauren Koller from NERC who will assist and help Joe Bucciero on the ready talk and document displays.

The Standards Committee met earlier in December and approved the use of an informal comment period followed by a formal 45 day comment period. While comments are underway, NERC will be assembling the ballot pool.

NERC understands the new CIP will represent a sea-change and paradigm shift for the Industry and will require a comprehensive communication campaign. NERC will develop more formalized campaign. This was started in early December, 2009 by presenting to and working with the Operations and Planning Committee and CIPSE at their meetings. NERC will be holding a webinar- in early February 2010 with industry and will need the Team's help on this. In terms of the CIP 003-009, security controls framework for development, NERC is hoping to have a better sense following the January SDT meeting in Tucker. NERC wants to give adequate support so the SDT can get this job done with a quality product. He asked the Team to continue to help NERC understand what is needed and NERC will seek to put tools in your tool box to help you.

The Chair welcomed and introduced Barry Lawson with the National Rural Electric Cooperative Association (NRECA) and current chair of NERC's Critical Infrastructure Protection Committee (CIPC). He noted the five trade associations that signed the letter to the SDT including NRECA, the Edison Electric Institute, the American Public Power Association, the Electric Consumers Resource Council and

the Electric Power Supply Association. He addressed the SDT not as CIPCE chair but with his NRECA trade association hat. He made remarks to Operations Committee, Planning Committee and to CIPSE last week. He offered to provide any support that the trade association could in support of the industry's self regulatory model and industry developed standards. He noted that the work of SDT is being closely watched by FERC and Congress and that it is getting more attention than a normal SDT usually gets.

NERC has reached out to trade groups to help the SDT. He asked the SDT to let them know what they can do to help. He believes the Industry has to demonstrate that we can develop the CIP on expedited basis resulting in a clear and objective way that is easily auditable for both entities and the auditor. He offered the following points:

- We must seek to eliminate subjectivity as much as possible from both a technical and political standpoint.
- The SDT should identify the "brightest lines you can come up with".
- Trade associations are not suggesting how to do this. The current draft has made huge steps in the right direction.
- If we don't get the CIP standards right there will be real consequences for the Industry including a potentially reduced role in the development of these standards. More is at stake than simply a ballot that doesn't pass with sufficient Industry support. Draft legislation is already out there that points in this direction and we have to show that the Industry can get the job done with our self-regulatory model which may not always the prettiest, but it promises to produce the best results for reliability and security.
- Please continue your efforts- this team has put much time and effort into this so far. Getting CIP 002 right is critically important. Bold steps are needed.

The Chair then welcomed and introduced Allen Mosher representing the American Public Power Association (APPA)**.** Mr. Mosher noted he was wearing two hats in addressing the SDT: one as a national trade association representative; and another as vice chair of the NERC Standards Committee. He recounted the NERC Standards Committee's review and discussion regarding the SDT process modifications for an expedited schedule and noted they came to consensus in support of this approach because of the shared understanding that the Industry needs to move expeditiously in revising the CIP. Hopefully we will get to consensus with industry on the new CIP and the industry is confident that you are listening to their concerns and you have a plan of action to address them. The joint Trade Association letter demonstrates this. He then offered the following points:

- The SDT's framework for the CIP appears sound and makes intuitive sense. Develop asset classification that will make sense to the industry.
- The Standards Committee stands ready to help the SDT in this important effort.
- In terms of the trade associations, we pledge to try to get our respective members to give early, responsive and constructive comments to the SDT on its drafts. We can also help to get subject matter experts focused on this project. Both in January for reviewing the CIP 002-4 and further on in terms of security controls (CIP 003-009)
- Need to know up front of problems. Will motivate members to get those to the SDT as early as possible. Let's get the right solution for the CIP suite of standards.

On behalf of the SDT, the chair noted appreciation for the work and efforts of NERC and the Trade Associations in assisting the SDT in its efforts to draw up a new CIP.

SDT Member Comments:

- How much preparation will it take for industry to understand this new approach? Is leadership preparing the industry for added expenses these changes will require?
- Mr. Lawson responded that he was reaching out to electric cooperative leaders- explaining the reality of the situation, i.e. that more and stricter standards will require greater costs and investments. While they are not offering the SDT a blank check, they do want to see the connection with costs and increasing effectiveness. Will reach out to NREECA members to provide them with context about draft and encourage them submit comments (both pro and con) early.
- Mr. Mosher noted that the APPA envisions similar efforts with its members. There will undoubtedly be push back on increasing costs as budgets everywhere are tight. However, capital expenditures are needed as the status quo is not sustainable. Now it is not whether, rather what changes are needed.
- Concerned within industry- undercurrent of members- any increase in compliance risk no matter how good it may be for security is a tough issue. Concerned the industry may vote against a new CIP because of cost implications. We need an outreach effort to National Public Utilities Commissions- by NERC. Mitigating security risks should also minimize "compliance risks" This will cost more money.
- As a result of recent NERC spot checks, the industry and the SDT are gaining a new appreciation for importance of words and their interpretation in the standards.
- Concerned industry will throw this back on us.
- Mr. Mosher noted that Gerry Cauley new CEO for NERC has championed an ad hoc committee on results-based standards and may be interested in developing a new format for how standards are developed and presented. Moving away from the compliance focus on the "right document" to real security issues. The test should be does the effort accomplish the underlying goal and intent of requirements. That should suffice.
- Probably not bringing the results-based effort into this project. This will be an ongoing effort. It will be a cultural change in NERC and the Regions that this is sensible way to process.
- State commissions are important outreach audience for NERC.
- The Trade Associations will do their best to provide context and the consequences as well as the big picture to their members. Each entity will ultimately decide where they are on this. We can't tell them how to vote, but we can provide information to inform their vote.
- Emphasis on getting it right this time? How will you know if you met this goal? How will you convince the skeptic in DC if you meet this?
- What about trials or pilots with entities? Is this still an idea in play? Having some since you've hit target.
- No exact way to know if you have it right. If you address some of these concepts- more objective, clear, deterministic and auditable, that will get us there.
- A substantial list of "wrongs" can help focus on the right thing to do.

- Concern that Industry won't accept the CIP as proposed. The industry needs to understand the consequences. We will have only one shot at this. More true now than before.
- Mr. Adamski noted that NERC President, Gerry Cauley has said this is among the top 3 things NERC needs to do.
- Spot check experiences suggest that there may be an unreasonable level of detail applied to enforcing current standards.
- Approve an increase in scope while compliance level of detail currently applied.
- We have seen an undue level of detail in policy documentation for CIP 003-R1- policy must support the requirements. Regional auditor went through every R looking for that. "All" does not appear in the requirement. Auditor used that tact.
- CIP 002- R3- critical cyber assets- e.g. given assets used in access control.
- CIP 004 issue- haven't provided in format the auditor wanted to see. Spreadsheet wasn't completed. Had all the info. This is an e.g. of audit and compliance out of control.
- Consider challenging finding of the audit? We have that process. One way to bring to attention of regional entity, NERC and FERC. Maybe indicate a problem with a standard.
- Can change to focus of the audit and how performed through the Version 4. As rest of standards become auditably compliant. Been on 14 CIP spot checks. In some suggested entities should do a better job of correlating.
- Trade association could help show that industry has valuable assets and they are trying to protect them.
- Trade associations are working together. 12 associations are marching together, educating various committees, various senators. Meeting weekly in Washington.
- Our focus should be on drafting standards- making them better- not on managing compliance risk. Focus on where we can make standards as clear as possible.
- Thanks for the help given. And support provided.

II. CIP 002-4 STRAWMAN DRAFT DOCUMENTS

A. Overview of CIP 002-4 Strawman Draft Documents

John Lim provided an overview of the work undertaken and the changes made to the CIP 002-4 draft documents between Orlando and Little Rock by a drafting group comprised of John Lim, Jackie Collett, Phil Huff and John Varnell. These included the CIP 002, the Guidance Document, the Introduction and Comment Form and the Control examples.

Dave Taylor noted that Howard Gugel from NERC will help the SDT get next products up to speed and be able to work with the SDT to answer any questions regarding format.

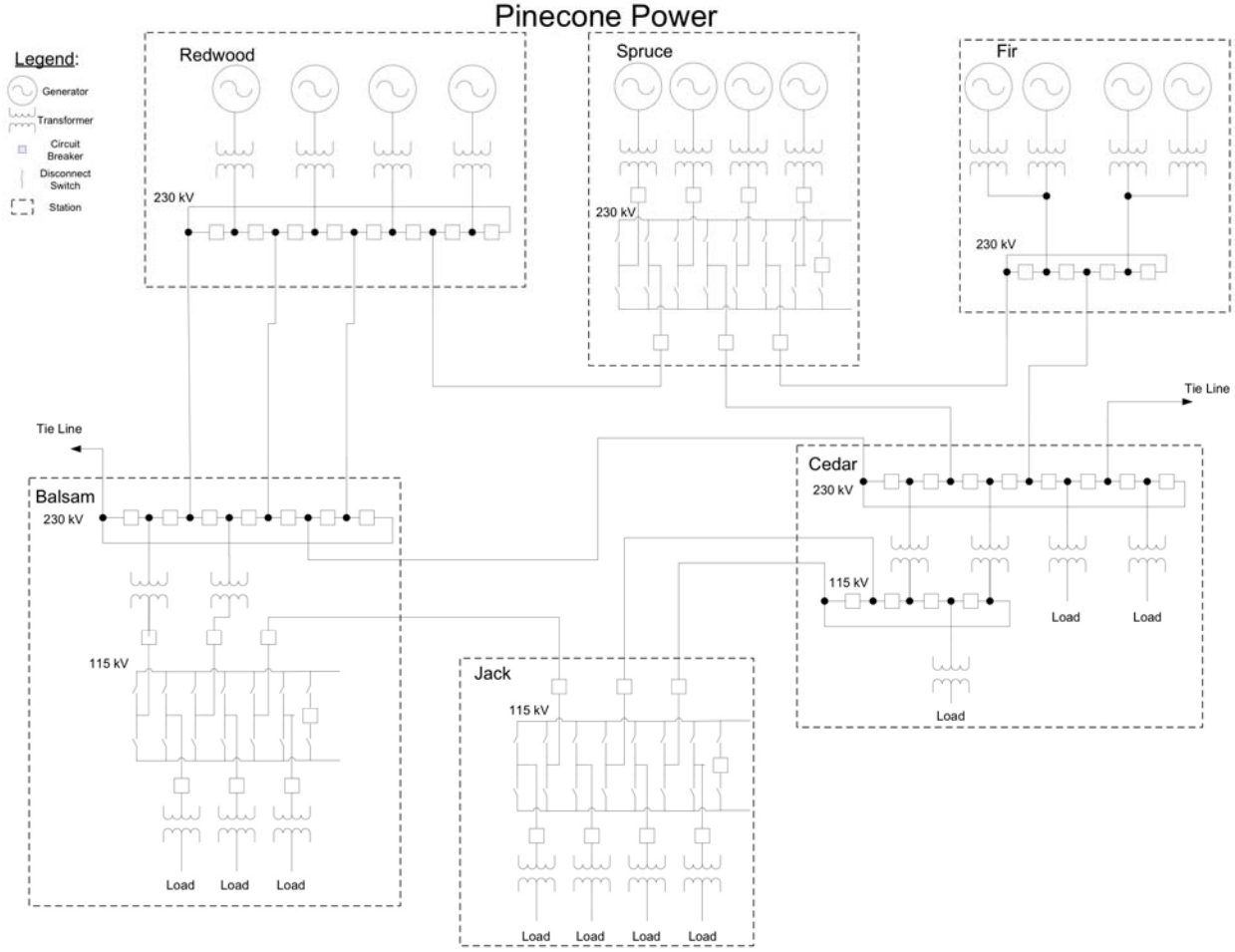
John summarized the following changes:

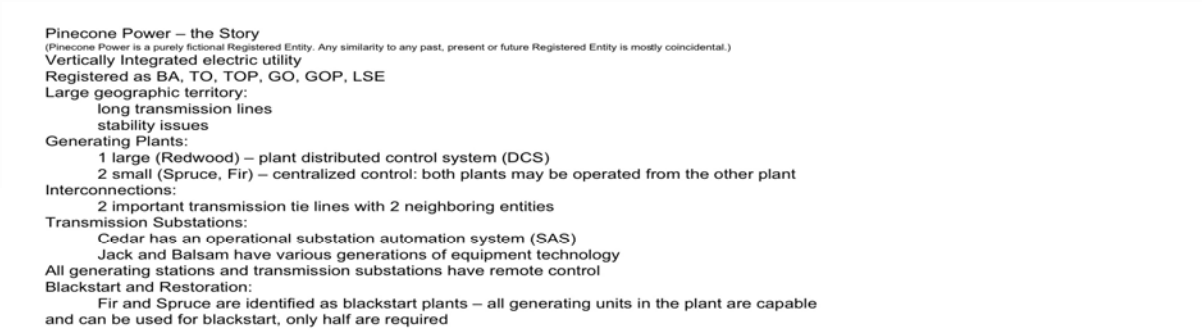
- A BES subsystem definition-
- Changed order of appendices. Harmonized- consistent use of terms.
- The list of the VSLs updated and some were put back in.

- The Guidance document has been refined and simplified with a 5-step process.
- We continue to need guidance in first two steps in categorizing BES subsystems.
- Agreed we will post as an "appendix" if ready.
- Highlights requirement. Tells the path to the development of the standards.
- Keith will be refining and cleaning up some examples for security controls as a stand alone document.

B. Walk-Through of CIP 002-4 Strawman Scenario

Jackie Collett provided an overview of the Pinecone Power "walk through" exercise.





Pinecone Power – the Story
(Pinecone Power is a purely fictional Registered Entity. Any similarity to any past, present or future Registered Entity is mostly coincidental.)
Vertically Integrated electric utility
Registered as BA, TO, TOP, GO, GOP, LSE
Large geographic territory:
long transmission lines
stability issues
Generating Plants:
1 large (Redwood) – plant distributed control system (DCS)
2 small (Spruce, Fir) – centralized control: both plants may be operated from the other plant
Interconnections:
2 important transmission tie lines with 2 neighboring entities
Transmission Substations:
Cedar has an operational substation automation system (SAS)
Jack and Balsam have various generations of equipment technology
All generating stations and transmission substations have remote control
Blackstart and Restoration:
Fir and Spruce are identified as blackstart plants – all generating units in the plant are capable and can be used for blackstart, only half are required

The SDT broke into two small groups and engaged in a "walk through" exercise that has been prepared by Jackie Collett, Dave Revill and other members. Following the breakouts, the SDT reviewed reflections on lessons learned from the walk through in terms of implications for improving or clarifying the CIP 002 draft.

1. **Possible Refinements to CIP-002-4**

- BES sub system definition - limitations <-> Reliability
- Clarify how to define BES sub system in requirements and/or guidance
- Determine Appendix 2 requirement in standard
- Clarify blackstart units that change - How to address this in requirements? "blackstart capable"
- Generating subsystems — define "Plant" — Units, combinations
- R1 — "Identify + Categorize"? vs. Categorize
- Keep cyber for R3? Not in R1 — rely on applying criteria
- How to address "combinations" in the subsystems? Start with cyber systems first?
- Appendix #2 "Must Identify" a requirement with appendix

2. **Key Issues — "Parking Lot" for Future Review**

- More detail on reliability functions to make operational — Address "Over Protection" issues — Map reliability functions to thresholds
- More specificity in reliability functions to allow entity to move description down in their operations — a cyber system may impact reliability but not the threshold — example a system

addressing operation awareness — make sure systems functions appropriately mapped to thresholds.

3. SDT Discussion Points from "Walk-Through"

- Did you identify the 7 generation subsystems? Some only came up with 6 but got to the right point. Will missing an interim step result in a severe impact?
- Goal is to categorize the cyber subsystems
- Careful we do not oversimplify categorization which may result in over protection — too many shortcuts could lead to incorrect conclusions
- Here is a cyber system — how many units does it impact - Look at megawatt total to set threshold of high-medium-low
- Think looking at units is the wrong path
- Break down to level of criteria you are evaluating — aggregation of megawatts at subsystem level— blackstarts would be at the unit level.
- Need a full assessment without requiring more work than is necessary
- Using generation subsystem across the board in the criteria — instead we may want to spell out generation subsystem or blackstart unit to make it clearer on to apply the criteria
- If pin down what we are talking about then replacing undefined subsystem with other terms that are undefined — new set of work to properly define and make sure each term properly used.
- We want to be sure nothing is missed — doesn't matter how it is defined if it is covered — then can choose to make it a subsystem but are not required to
- Give entities flexibility but careful don't leave an opportunity to game system by breaking systems into parts that stay below threshold for "high"
- No individual generator can determine full impact on system — that may require RC to determine but they will not want to do that task
- Clarify something in R3 — identify and categorize all BES subsystems ….. that means identify every part of cyber system that has anything to do with awareness function — is that what we meant?
- Every cyber system that performs that function should fall into one of the three categories, each with its own threshold
- How do you start — where do you get the list? Situational awareness is the universe of all cyber systems
- My take, we are saying you have to do the functions — which are BES cyber systems — every BES cyber system is at least a low based on the words we use here
- Maybe by extending the logic, you get around identifying subsystems — any system that can trigger specific levels
- Instead of starting with every cyber system — identify every cyber system that supports this BES subsystem

4. SDT Discussion of Next Steps in Drafting CIP 002-4

- Next steps in drafting?
- Build into R3 concept discussed in terms of the function of the BES subsystem
- Unclear where discussion of generation subsystem ended up — did not discuss transmission subsystems
- In criteria we can try to be more specific
- We may need to have very formal definitions we can put into the NERC glossary
- What is missing is what is the objective — should we try to introduce each requirement with the objective to help focus comments on what we are trying to do
- Can put that into the purpose statement to help clarify intent — that puts it into the standard — NERC has used those statements in the past to help in interpreting intent
- For the comment period, can we use statements as annotations to introduce a requirement?
- Scott read Maureen's revised purpose statement
- Members thought it sounded like she is trying to move to performance based standards, but this group may not be ready to do that given the limited time
- Adding more material may just draw comments on statements that will not be included in the end (relates to introducing requirement with intent comment)
- Suggesting a one-sentence introduction to clarify the intent and context of each requirement
- Could something be added to the comment form to set up the questions?
- Need more drafting input on appendix 2 — review the wording of the initial paragraph to avoid requirement language in the appendix

C. Remaining Issues

1. Small Group Work on Requirements # 1 and # 3.

Following the Walk Through, the SDT reviewed the remaining issues and agreed to work in the following Drafting Groups on Wednesday afternoon to address issues raised in the "Walk-Through" and bring back clarifications and refinements for consideration by the SDT.

- Group #1 Requirement #1 (*Jim Brenton, Jackie Collett, Keith Stouffer, Doug Johnson, Jeri Domingo Brewer, John Lim)* which reviewed and produced agreement on how to address the R1 and appendix issues raised in the walk through.
- Group #2: Requirement #3 drafting group (*Phil Huff, Jay Cribb, Frank Kim, Jon Stanford, Gerry Freese & Jeri Domingo Brewer)* How will this be understood- i.e. smaller unit is more secure than securing with a larger quantity. We are not trying to avoid protection; rather we are trying to determine how it affects the BES. Collectively assets may have a higher impact than one large asset.

At the end of the day, the SDT reviewed progress and noted the following assignments:

- Issues of reliability functions— Phil Huff noted a plan to meet for dinner and resolve these issues and bring suggestions back tomorrow first thing tomorrow.
- Break into groups for document drafting (introduction and comment form; CIP 002-4; Guidance Document; Appendices; and Sample Controls.

Chair reminded the SDT that the goal is to ensure posting for informal industry review and the SDT should expect many suggestions back from industry. She also checked with the SDT to see if there were any red flags on proposed list of FERC specific directives in 706 since it will be part of the NERC filing at the end of December. The SDT concurred with the list.

2. Definition of Terms

On the second day John Lim reviewed with the SDT the revised definitions of terms used in standard noting:

- #3 Bulk Electric System spelled out.
- generation subsystem turned from a bulleted list into a paragraph.
- transmission subsystem defined more specifically
- control system, second bullet added the qualifier "for the support of real-time operations"
- 7, 8 & 9 — changed to "BES" to be consistent — 9 adds Low BES impact

SDT Discussion of Proposed Changes to Definitions

- All the other bulleted lists turned into paragraphs — Is #9 the only bulleted list?
- #8 — does "medium" capture everything?
- High, medium and low are not intended to be used to capture categories but criteria — pulled from risk factors — be sure not to use definitions to apply categorization — does defining a term here make it apply in the standards?
- If leave it in then indicate how they are to assess the high, medium and low.
- Do we want them here in definitions versus in the attachment?
- Let the attachment determine rather than define them?
- Inclined to take it out of the definitions — this issue is even fluid at NERC — leave it in the attachment.
- Define here and reference the attachment? If put in to the standard, once adopted it goes into the glossary.
- Bring definition up to a higher level with the detail in the attachment?
- Is there an inconsistency between this and the mapping? What is wrong with this definition? Conflicts with the mapping, according to the definition here everything is high or medium, and nothing is low — everything affects the BES.
- Cannot read the bullets alone — have to read in context of lead-in language.
- All of them affect the system — the question is only how much they affect the system.

- Define BES impact — then categorize that with high, medium and low as degrees for measuring the impact.
- Suggestion changing "direct" to "adversely" in each bullet.
- Either simplify this or do not make missing one a high VSL — too complex to make it a high VSL if you miss one.
- High VSL is related to the importance of missing one rather than the complexity of the standard.
- Make sure we have the detail in each thing we are doing — make it too simple then people will complain it is ambiguous.
- Last sentence of Generation subsystem — confusing with a transmission issue — consider adding "... shared generation element …"
- What is a "generation element" — both generation and element are separate defined items — is this just the generator?
- Non-capital "generation" simply describes "Element" — the latter is a defined item, the former is not.
- Elements at a generation yard, etc. — clarify that we are not talking about something that doesn't spin.
- Is the last "or…" clause intended to capture something not already captured in the cyber system definition?
- Jackie Collett's revised definitions of Generation and Transmission Subsystems — review — it is a little wordy but it is more specific — included transmission substations in the later definition
- "Combinations of generation systems"? — not clear what that covers — could be more open than needed — need a qualifier for "combinations"
- Strike the last section of the first sentence — add "or" — should read "Generation plants or individual generation units … a transmission system."
- I don't understand the second sentence — how would it be applied?
- Combine the last two sections into a final separate sentence?
- Does generation plant mean everything inside the fence? Thought we had dropped that?
- Put in as part of the walk through review yesterday — the "or" gives the entity a choice
- Are elements in the second sentence already covered in the first? Or do we need the first sentence if the elements are covered in the second?
- In terms of the definition, is it redundant? Start with the second sentence?
- Concerned we may miss something if we take the first sentence out — would rather be redundant than miss something
- Transmission definition is closely parallel with generation — same issues — consider issues for both, move on for now and come back to this one.

3. Review of Changes to Standards Section

Phil Huff led the SDT through a discussion of the changes to the standards section.

- **R-1.** Purpose statement — shorter, more focused
- Identifying cyber security framework or the devices that require security?
- Consider just using the last paragraph of the previous definition version
- Up in the title — strike "identification and" — just categorizing, not identifying — remove "identification" in the purpose too
- Add "functions critical to the reliable operation" to the Purpose to be consistent
- Strike first set of words and start with "categorization" to make it a purpose statement rather than a requirement statement — start with "To categorize and document the BES …"
- #3 Applicability
- #4 Physical Facilities

  Insert "and are not under NRC cyber security regulations" at the end?
- Suggest not adding yet due to ongoing discussion of jurisdiction — balance of plant is still under NERC — following comment period the jurisdiction issue may be clarified — may get comments form nuclear guys.
- R1- Drop "serves" in first sentence "…BES subsystems provides a measure …"
- Add "...potential impact that its …"
- "Approved engineering evaluation" required? (in middle sentence) Method has to be approved but not every yearly evaluation is approved.
- Second sentence is long and wordy tighten up, along with the third sentence — if we can get agreement on the elements.
- Fiscal responsibility is with the owner — some facilities have multiple owners (by percentages) asking all owners to make the assessment?
- Who signs compliance? Operator not always the one who can ensure compliance — some plants have a contract operator — need to include "operators and owners" Owners should "ensure" — put them on the hook to make it happen.
- Reduce wording by striking "categorize all BES subsystems they own: and own …"
- The responsibility issue is a registration issue.
- Joint ownership issue is not new — how do we do this in the other standards? What is the language we used? We used to have a definition of "responsible entity" but stripped it out — the idea is be clearer about responsibility — spell out the entities in each requirement — some requirements may not be mapped to entities (?) — may have to go back through and clarify responsibilities
- R1 final sentence: "could affect" is too mushy, too uncertain
- Some want to put the "annual" requirement back in and some who want to take it out.

- TPO requirements call for "annual" evaluation. Need to make clear what we mean by "annual." The issue of "annual" appears in multiple places and on multiple projects. Need to be sure it is applied as part of review process — may want to wait for comments.
- **SDT Poll support for reinstating "annual" term in the standard for draft for comment: Yes — 8, No — 10. Won't reinstate for CIP 002-4 draft.**
- **R2-** Notification from generation to transmission side of the house a "high"?
- How does generation subsystem owner learn he has a high or medium? By definition or someone (reliability coordinator) tells him?
- Needs to be a clearer delineation of notice, and should be a "high" responsibility
- The owner has to determine through criteria, not the reliability coordinator who do not have any special ability in this area
- Look at attachment 1 — there are instances when owner operator will be notified — it is not just one or the other
- This is one of the places that industry has a problem — not enough of a bright line — owner/operator may not have enough data to assess
- "adjacent"? Replace with "connected to"? And specify the within 30 days is from R4?
- Adjacent is physical proximity — connected is the better word
- Add "…within 30 days of the approval date of the categorization …"
- Change "connected" to "directly interconnected"
- Why include "Senior Manager"? Addressed FERC directive. Need to look at the order — careful not to do more than is requested in the order.
- Is there a definition of "Senior Manager"?
- Why thirty days? Seems lengthy and arbitrary
- R4 already has the language of who approves — drop it here
- Is R4 necessary if we are dropping Senior Manager? Address when review that section.
- Suggest "within 30 days of the categorization" - 30 days is not too long to get ducks in a row.
- Violation risk factor should be "high".
- In R2 can we make it a "secured notification"? Define "secured"?
- Back to R1 to review revisions
- Do we have to list them all to add clarity to the definition? Add load serving entity and reliability coordinator.
- Need to go back and see what the functional model says — or post all and ask which entities do not belong — alternatively list all entities in 4.1 except NERC and Regional Entities
- Requiring reliability coordinator to assess others systems — goes back to ownership — reliability coordinator has no special skills to assess cyber security systems
- Can we change to cover own and operate?

- Is the control center considered a subsystem? If yes, as part of the BES subsystem, it is not clear hear where it is covered
- Put into the definition of control center that it may be a part of the BES subsystem
- In definition of BES Subsystem include "BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center)…"
- **R3**. Phil Huff reviewed revisions with the SDT
- 2nd sentence — do we need the final clause?
- Is our intent to identify or to categorize? Intentionally pulled "identify" out of R1 — are we being consistent?
- Remove "as those …" replace with "associated with" — also "Responsible Entities shall categorize" and put "… categorized in R1..."
- Planning function is both and internal and external — copy "… as part of the planning, including coordination with neighbors," from the R1 revision and use here too.
- Not requiring notification of our neighbors?
- Delete the final sentence? Not part of the security but better as part of control.
- Are we overloading the meaning of the term "planning" — we used it in sentence above with the normal NERC definition.
- Beginning of second sentence — Functional Entities and again in third and fourth sentences rather than Responsible Entities —
- Functional doesn't work here — need to go back to responsible.
- Need to capture changes in BES subsystems as well as BES cyber subsystems
- **R4**. Is the senior manager the right one for this role? If not, then does this requirement do much? Support removing.
- If remove, are we removing responsibility for person knowing what was happening.
- Despite the language in the FERC order paragraph 294, I think FERC would still want senior manager here explicitly because we have changed the process since their original request — I suggest leaving R4 in.
- Change "shall approve by written and dated signature" to match order "shall annually review and approve"
- The point was to establish a fiduciary duty to take responsibility and make a knowing effort to establish what was and what was not covered — now we have said everything is covered, but at three different levels.
- Approving additions or improvements to the system or annually reviewing the whole system?
- Ask in the comment form whether we need this requirement?
- Here we have prescribed the methodology — we responded to the order by changing the methodology.
- If we put it out as a question we need to get a response from FERC too

- FERC asked us to address regardless of the industry comment
- Leave it for industry comment and pose question for clarification with FERC
- Does senior manager necessary mean corporate office?
- This section is about categorizing assets, not putting in weak controls better addressed in 003-009
- My advice from other standards — if remove, better be sure you have a clear rational and suggestion of how it will be dealt with
- We need to be rethinking here and my concern is the senior manager shall is a weak control in the wrong place
- Intent of pulling senior manager into the process is to give it the attention it needs — establishes accountability as to what needs to be protected to big with — controls will be addressed next year
- This says the right thing, maybe in the wrong place, but pulling it out of here now will result in perception we are not addressing the issue
- Violent agreement on importance — question is where? It magically appears in R2 as a capitalized item without definition in R1.
- Three thoughts: any of these acceptable? (rather than one or the other).

  Members offer the following responses (multiple votes were permitted):

  - Remove it, address it elsewhere: 10 votes
  - Keep in R2 but with fuller definition: 9 votes
  - Keep it here as is: 7 votes
  - Remove here and keep in the comment form: 1 vote

  Members then offered the following preference polling *(only one vote of one of 3 options)*

  - **Remove it, address it elsewhere: 8**
  - **Keep in R2 but with fuller definition: 5**
  - **Keep it here as is: 1**
- There is consensus of the importance of the issue and inclusion of the senior manager but less clear how best to do it.
- Since removing it here now, need to clarify why
- Back up in R3- Strike "responsible entity shall" and rest of the last sentence. Still needs a tie back to R1 —

4. Review of the Revised Definitions for BES, Generation and Transmission Subsystems

- Still questions about discussions by nuclear industry and the impact on these definitions
- Definitions 7, 8 & 9 — High, Medium & Low
- Consider reorganizing the criteria based on H-M-L and by generation/transmission
- Remove "details provided in appendix 1" — put in above #7 — re-label as "attachment"

- Don't put that language in the definitions — it will be lost once adopted and moved into the glossary — each will stand alone in the glossary
- Not meant to be a part of the definition but rather to help clarify and explain for purposes of the comment period
- May need to consider for the next round given our time constraint today
- This doesn't include malicious use of the equipment, not just lost
- Doesn't matter if loss is by natural or malicious means — source of loss doesn't matter
- Perhaps include "misused"
- Need a more clear cut, declarative sentence
- These terms will be used independent of CIP 002
- Rewrite to be declarative: "BES Subsystems, that if destroyed….would have a severe….change #8 and #9 accordingly
- Concerned about "destroyed", etc. — concerned about availability — remove adjectives — doesn't matter how they are rendered unavailable — simply substitute "rendered unavailable"
- It is more than just availability — integrity matters too in cyber security
- Just looking at BES, not cyber security yet
- Need "misuse" — adds more than just availability — "that if misused, degraded or otherwise rendered unavailable…"
- Need to be describing the impact to the BES
- For now go with suggestion to go with previously adopted language — put the issue into the parking lot for future work

5. Compliance

- No changes were made to this section.

6. VSLs

- #1
- Made consist or conformed with discussions and changes made earlier today
- Still concerned with high impact given a severe VSL for not having categorized or mis-categorized
- Whole point in attachment and drawing bright lines is to limit auditor opinions on categorization
- Concern is with definition of subsystems
- We are only left with categorization — only have to categorize rather than identify subsystems
- In severe VSL — kill the phrase after "or" and put a period after "categorized" in all four levels?
- Just eliminate "identify" — retain the rest
- Should say has failed to start the process

- If you missed any single one by saying there are six subsystems and someone else says there are seven — am I then in severe VSL?
- Alternative: "The responsible entity has not categorized any BES subsystems it owns". Support for this language — Yes/13, No/1
- **#2**
- Too wordy — repeat high and medium impact at the beginnings and ends — could strike first half of each.
- Only two ways to miss — not notify or notify late
- **#4** — already removed

7. Attachments

- 1.3 — ok
- 1.8 — ok
- 1.15- Interchange coordinator, transmission service provider, load service provider, selling entity, etc. all have real time function responsibilities — none of them will be caught by 1.15?
- Can we expand 1.7, 1.10 or 1.11 to cover that omission — put control center functions into those three

8. Other Changes?

- What did we do with the requirement for VSL 2? Everyone agreed with concept just need appropriate language

D. Motion to approve CIP 002-4 with identified and agreed upon changes
Gerry Freese moved, John Varnell seconded

All in favor: **16** *(Frank Kim, Doug Johnson, Sharon Edwards, Gerry Freese, Jay Cribb, Keith Stouffer, Jon Stanford, Jim Brenton, John Lim, Jeri Domingo-Brewer, Phil Huff, Joe Doetzl, Rob Antonishen, John Varnell, Jackie Collett and Kevin Sherlin)*
Opposed: **0**
Abstain: **1** (Dave Norton)

E. Harmonizing the Comment Form and Guidance Documents

Following a break, the SDT broke into separate "document" groups to harmonize the comment form and guidance document with the adopted CIP 002-4:

- **Introduction and Comment Form**: (Frank Kim, Jay Cribb, Jon Stanford, Jim Brenton, Jeri Domingo-Brewer, John Lim, and Keith Stouffer, Jackie Collett, Dave Norton, John Varnell and Rob Antonishen)
- **Guidance Document**: (Phil Huff, Gerry Freese and Doug Johnson).

At the conclusion of the small group refinements to these documents the SDT reviewed the following key issues for the future (i.e. "parking lot")

- More detail on reliability functions to make operational — address "over protection" issues — map Requirement Function to thresholds
- "Controls" — "secure" defined — address in 003-009
- "BES Subsystem Impacts" define going forward (high/medium/low)
- 1.7, 1.11 & 1.15 — control center function issues)

IV. NEXT STEPS

The SDT Chair and Vice Chairs reviewed with the Team the work plan going forward including the need to make progress on the security controls (CIP 003-009) at the SDT's January meeting in Tucker, Georgia. The chair thanked Phil Huff for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 3:30 p.m. on December 16, 2009.

Appendix # 1— Meeting Agenda

NOTE:

1. Agenda Times May be Adjusted as Needed during the Meeting
2. Document Drafting Group Meetings May Not Have Access to Telephones and Ready-Talk

Proposed Meeting Objectives and Outcomes

- Receive an overview the CIP 002-4 document drafting progress
- Conduct a walk-through of the CIP 002-4 and identify lessons learned and any changes needed in the document(s).
- Review CIP 002-4 Key Issues and Provide Guidance to Document Drafting Groups
- Convene CIP 002-4 Document Drafting Groups
- Review and refine Document Drafting Group products
- Compile, review and refine the draft CIP 002-4 and related documents
- Adopt the CIP-002-4 Documents for Posting
- Review CSO 706 SDT leadership changes
- Review the 2010 Schedule and agree on next steps and assignments

Tuesday	**December 15, 2009**
8:00 a.m.	Welcome and Opening Remarks- *Jeri Domingo Brewer, Phil Huff & John Lim* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of November 16-19 Orlando SDT meeting summary
8:15	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
8:20	Review of SDT 706 Work plan- December- June, 2009- *Jeri Domingo Brewer*
8:50	Overview of CIP 002-4 Strawman Draft Documents, Format and Key Remaining Issues and Challenges- *John Lim et al.*
9:15	Walk Through of CIP 002-4 Strawman Scenario-*Jackie Collett, Dave Revill et al.*
10:30	*Break*
10:45	Reflections and Lessons Learned from Walk Through and Implications for the Draft
11:15	Run-through and Flag Key Remaining Issues in CIP Version 4 Strawman Documents
12:15	*Lunch*
12:45	Review of Remaining Issues and Proposal for Drafting Groups
1:00	Drafting Group Meetings
4:00	Drafting Group Reports and Identification of any Outstanding Issues and Drafting Assignments
5:30	*Recess*

Wednesday	**December 16, 2009**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer, Phil Huff & John Lim*
8:10	Update on Status of Version 3 CIP—*Scott Mix*
8:15	Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure —*Scott Mix*
8:20	Update on VSLs/VRFs- *Scott Mix*
8:25	Update on other related cyber security initiatives- *SDT Members*
8:30	Reconvene SDT CIP 002-4 Document Drafting Groups *(as needed)*

10:30	Break
10:45	Final Document Review and Consensus Testing on Resolution Key Remaining Issues
12:00	*Working Lunch (compilation of refined CIP 002 documents)*
12:45	Review of CSO 706 SDT Leadership Changes
1:00	Final Document Review and Consensus Testing on Resolution Key Remaining Issues
3:00	*Break*
3:15	Final Document Review and Motion to Adopt as Refined for Industry Posting
4:30	Review and Agree on CIP 002-4 Next Steps and January- June Work plan and Schedule • Meeting Evaluation
5:00	*Adjourn*

Appendix # 2 Attendees List

Attending in Person — SDT Members and Staff

1. Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
2. Jim Brenton	ERCOT
3. Jay S. Cribb	Information Security Analyst, Southern Company Services
4. Sharon Edwards	Duke Energy
5. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
6. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
7. Doug Johnson	Exelon Corporation — Commonwealth Edison
8. Frank Kim	Ontario Hydro
9. Rich Kinas	Orlando Utilities Commission (Wed)
10. John Lim, Vice Chair	CISSP, Department Manager, Consolidated Edison Co. NY
11. Jonathan Stanford	Bonneville Power Administration
12.Keith Stouffer	National Institute of Standards & Technology
Roger Lampila	NERC
Scott Mix	NERC
Dave Taylor	NERC
Howard Gugel	NERC
Lauren Koller	
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center
Gerry Adamski	NERC (Wed.)

SDT Members Attending via Ready Talk and Phone

13. Rob Antonishen	Ontario Power Generation (Thurs)
14. Jackie Collett	Manitoba Hydro (Wed/Thurs)
15. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co. (Thurs.)
16. Rich Kinas	Orlando Utilities Commission (Wed.)
17. David Norton	Entergy (Wed. Thurs)
18. Kevin Sherlin	Sacramento Municipal Utility District (Wed. Thurs.)
19. John D. Varnell	Technology Director, Tenaska Power Services Co. (Wed. Thurs)

SDT Members Unable to Attend

Christopher A. Peters	ICF International
Scott Rosenberger	Luminant Energy
David S. Revill	Georgia Transmission Corporation
William Winters	Arizona Public Service, Inc. (Mon., Tues, Thurs)

Others Attending in Person

Alan Mosher	APPA
Barry Lawson	NRECA

Others Attending via WebEx and Phone

Rob Hardiman	Southern Company Transmission
Joseph Baxter	AECI
Justin Kelly	FERC
Justin Kelly	FERC
Michael Toecker	Burns and MacDonald Engineering
Bill Glynn	Westar Energy
Sam Merrell	Cert
Rob Wotherspoon	Orlando Utility Commission
Michael Fischette	LBWL
Laurel Moll	Orlando Utility Commission

Appendix # 4 — 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 Subroups) 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 Subgroups) 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 Subgroups) 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 Subgroup, 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 Meeting Schedule

OCTOBER 2008—DECEMBER 2010

DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008—JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.

- January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
- January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

- *March 2–April 1, 2009 — 30-day Pre Ballot*
- *Mid-March — NERC posts TFE draft Rules of Procedure for industry comment*
- *March 30, 2009 — WebEx meeting(s) White Paper Drafting Team*
- ***April 1–10 — NERC Balloting on Version 2 Products***
- *April 6, 2009 — WebEx meeting — White Paper Drafting Team*
- *April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call*
- *April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments*

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

- *April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx*
- *April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%*

- *May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.*

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada
SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010
September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)
- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002 for industry review and comment.
- Agree on next steps and 2010 Work plan and schedule

Refinement and Adoption of CIP-002 Version 4 and Development and Adoption of CIP Standards (003-009)
January 2010–December 2010

18. January 19-20–21-22 — Tue-PM- to Friday AM, Tucker, GA (GTC)

- SDT Work on Developing CIP 003-009 Strawman Drafts

19. February 17-18–19 —Wed--Thursday –Friday, Austin TX (ERCOT)

- SDT Reviews Industry Comments and Refines CIP 002 for posting for 45-day industry formal comment period.
- SDT continues CIP 003-009 Strawman Drafts

20. March 9–10-11 — Tuesday–Thursday, Phoenix, AZ (APS)

- SDT continues CIP 003-009 Strawman Drafts

21. April 13-14–15 — Tue-Wednesday–Thursday, Atlanta GA (Southern Co)

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting
- SDT posts a draft CIP 003-009 for informal industry comment.

22. May 11-12–13 — Tue-Wednesday–Thursday, Dallas TX (Luminant)

- SDT reviews Industry 1st Ballot Comments and Drafts Responses
- SDT reviews CIP 003-009 informal industry comments and refines the draft.

23. June 8-10- Tues, Wed. Thursday- (Sacramento)

- SDT refines CIP 003-009 and posts for 2nd round of informal industry comments and refines the draft.

24. July 13-14–15, Tue-Wednesday–Thursday, Pittsburgh, PA (CERT)

- SDT reviews CIP 003-009 informal industry comments and refines the draft.

25. August 10-11–12, Tue-Wednesday–Thursday- TBD

- SDT refines CIP 003-009 and posts for formal 45 day industry comment

26. September 7,8,9, Tues-Thurs. TBD (if needed)

27. Oct. 12-13–14, Tue-Wednesday–Thursday- TBD

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting

28. November 16-17–18, Tue-Wednesday–Thursday- TBD

- SDT reviews Industry 1st Ballot Comments and Drafts Responses

29. December 14-15–16, Tue-Wednesday–Thursday- TBD

Appendix # 6 Trade Association Memorandum to SDT

December 10, 2009

TO: NERC CSO706 Critical Infrastructure Protection Standard Drafting Team

FROM: American Public Power Association, Edison Electric Institute, Electricity Consumers Resource Council, Electric Power Supply Association, and National Rural Electric Cooperative Association (the "Associations")

SUBJECT: Support for Expedited Revision of NERC Cyber-Security Standards

On behalf of our Associations, we want to express our support of efforts now under way by the CSO706 Standard Drafting Team to expedite development of a revised set of cyber-security reliability standards, including consideration of a tiered approach to the identification of bulk electric system ("BES") assets under CIP-002-4. We understand that assets within each BES tier will in turn be subject to a new suite of cyber-security controls developed under reliability standards CIP-003-4 through CIP-009-4.

As you know, Congress and the Executive Branch have identified cyber-security of the nation's critical infrastructures as essential to the protection of the public welfare, national security and national economic security. Therefore, NERC and the industry now have the opportunity to demonstrate the value of industry expert participation and the effectiveness of industry self-regulation by delivering a timely set of consensus critical asset identification parameters. The Associations believe a new, more systematic approach to asset classification will best ensure that BES assets are subject to the appropriate cyber-security protection controls that are commensurate with their importance to reliable operations and their vulnerability to cyber-security threats.

The Associations are committed to working with their members' executives and managers, to ensure that industry subject matter experts provide timely and constructive comments on the scheduled December 28, 2009 posting of Version 4 of CIP-002, and subsequent balloting. We recognize the difficulty of drafting during the holiday season, the tight time frame for conducting a thorough revision on matters involving complex technical issues, and the prospect that this process could invoke considerable tension and disagreement on a broad range of issues. However, we offer our support because we believe it is important that the industry reach consensus on CIP-002-4 during the next six months and deliver a full suite of cyber-security

standards for approval by the NERC Board of Trustees by the end of 2010. Consequently, it is imperative that the identification piece of the process starts well, and remains on track.

The Associations recognize that there may be several alternative approaches for defining applicability of the standards. If approved as reflected in the conceptual framework, the tiered approach to BES asset identification would be a significant departure from the current approach to critical asset and critical cyber-security asset identification. Reaching an industry consensus in support of a new conceptual framework and developing a clear, complete and enforceable set of reliability requirements on an aggressive timeline will be difficult at best. Implementing a new framework raises significant cost implications that must be addressed as well. However, given the importance of the role cyber-security plays in ensuring a safe and reliable electric system, the work of your drafting team is in our view a crucial NERC project.

Therefore, we offer our strong support for the expedited timeline and consideration of the tiered approach and to provide our encouragement for completing by the end of next year the critically important tasks you are performing. We are committed to providing whatever personnel and other resources and support needed to accomplish this goal.

Contact Persons:

Allen Mosher
American Public Power Association
(202) 467-2944
amosher@APPAnet.org

James P. Fama
Edison Electric Institute
(202) 508-5725
jfama@eei.org

John A. Anderson
Electricity Consumers Resource Council
(202) 682-1390
janderson@elcon.org

Jack Cashin
Electric Power Supply Association
(202) 349-0155
jcashin@epsa.org

Barry R. Lawson
National Rural Electric Cooperative Association
(703) 907-5781
barry.lawson@nreca.coop

Appendix #7 CIP-002-4 Template
FERC Specific directives from order 706:

Compiled by Scott Mix, NERC

The following table contains the status of all issues raised in the order that were either "direct"ed, specifically in the order, or "adopt"ed from the NOPR.

Note: Given the confusion over the SDT's inclusion of the change in CIP-008 ("Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test") that the commission did not "direct", even though p 687 states: "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service," I did not include any issue that was not actively directed for change, such as those designated "should consider" or similar.

Issue #	Paragraph #	Text	Phase[1]
1	13	NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.	This compliance filing; and an implementation plan is filed with each submitted version of the standards
2	25	we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	Version 4
3	47	The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance with the CIP Reliability Standards.	Rules of Procedure statement
4	49	The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards	Compliance registry process
5	72	We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement.	CMEP
6	75	we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards	Version 2
7	86	The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities	CMEP

[1] Schedule phases in this column mean one or more of the following:
- "Version 2" – complete in filed version 2
- "Version 4" – planned for next major version (12-18 months plus)
- "Guideline" – stand alone guidance started after corresponding requirement is determined
- "TFE Filing" – 2009 filing on TFE proposal and Appendix 4D to RoP
- "not scheduled" – beyond Version 4
- "CMEP" – part of an existing or ongoing compliance audit, self-report or other process
- "VRF Filing(s)" – one of several already-filed (or very soon to be filed in the case of Version 2) VRF and/or VSL filings

Phase may also be self-explanatory if not one of these entries

Issue #	Paragraph #	Text	Phase[1]
		to achieve auditable compliance.	
8	89	we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule	This compliance filing; and an implementation plan is filed with each submitted version of the standards
9	90	We direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.	TFE Filing
10	96	we direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required	CMEP program and self-certifications
11	97	we adopt our CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify	CMEP, self-certification process
12	106	the Commission adopts the CIP NOPR proposals and directs NERC to modify the CIP Reliability Standards through the Reliability Standards development process to remove the first two Terms ["reasonable business judgment," and "acceptance of risk"], and develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception	Version 2 and TFE Filing
13	128	the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.	Version 2
14	138	the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.	Version 2
15	150	The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.	Version 2
16	156	the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.	Version 2
17	178	directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards	TFE Filing
18	186	the Commission adopts its proposal in the CIP NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place.	TFE Filing
19	192	the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address	TFE Filing

Issue #	Paragraph #	Text	Phase[1]
		mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception.	
20	209	The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria.	TFE Filing
21	211	direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.	TFE Filing
22	212	the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed.	TFE Filing
23	218	we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process.	TFE Filing
24	219	we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive information.	TFE Filing
25	220	We direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability.	TFE Filing
26	221	we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.	TFE Filing
27	222	we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards.	TFE Filing
28	222	We direct the ERO to develop appropriate modifications, as discussed above.	TFE Filing
29	233	we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission.	Ongoing discussions with Drafting Team Members from USBR, BPA, NIST; Development of Version 4
30	253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance … leave to the EO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	Guideline / Version 4
31	254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-	Guideline / Version 4

Issue #	Paragraph #	Text	Phase[1]
		Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary]when developing the guidance.	
32	255	we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.	Unscheduled
33	257	we direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Guideline / Version 4
34	272	the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Guideline / Version 4
35	272	The Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Guideline / Version 4
36	282	the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	Guideline / Version 4
37	285	we direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable — by testing and experience].	Version 4
38	294	The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
39	294	the Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
40	322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0
41	329	the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0
42	333	we direct the ERO, in developing the accountability structure for the	TFE Filing

Issue #	Paragraph #	Text	Phase[1]
		technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information	
43	355	the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address.	Guideline
44	376	the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 4
45	381	The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards	Version 2
46	386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 4
47	397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 4 / Guideline
48	412	The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.	Guideline
49	431	The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.	Version 2
50	433	we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 4
51	434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.	Version 4
52	435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made	Version 4

Issue #	Paragraph #	Text	Phase[1]
		to assure that security trainers are adequately trained themselves.	
53	443	The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency.	Version 2
54	443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 4
55	460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 4
56	464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 4
57	473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	Version 4
58	476	we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent	Version 4
59	496	The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter	Not scheduled
60	502	The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.	Not scheduled
61	502	The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline

Issue #	Paragraph #	Text	Phase[1]
62	503	The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures.	Not scheduled
63	511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 4
64	525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days	Version 4
65	526	the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 4
66	526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 4
67	528	the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 4
68	541	we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 4
69	542	the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 4
70	544	the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.	Version 4
71	544	we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment	Version 4
72	547	we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	Version 4
73	560	the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions.	TFE Filing / CMEP
74	572	The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around	Not scheduled

Issue #	Paragraph #	Text	Phase[1]
		critical cyber assets.	
75	575	The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline
76	581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 4
77	597	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2.	Version 2
78	600	Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility.	Version 2 / TFE Filing
79	609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	Version 4 / Guideline
80	610	we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 4
81	611	the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 4
82	619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	Version 4 / not scheduled
83	622	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2	Version 2
84	622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously	Version 4 / not scheduled

Issue #	Paragraph #	Text	Phase[1]
		or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	
85	628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	Version 4
86	629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 4 / guideline
87	633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.	Version 4
88	635	the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4
89	643	The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.	Not scheduled
90	651	We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days.	Version 2
91	660	The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. … we direct the ERO to develop and provide guidance on the term reportable incident.	Guideline
92	661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced	Version 4 / Guideline
93	673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the	Version 4 / Guideline

Issue #	Paragraph #	Text	Phase[1]
		event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	
94	676	the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 /. Guideline
95	686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.	Version 4
96	686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 4
97	694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 4
98	694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.	Version 4
99	706	The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.	Not scheduled
100	710	Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report.	Not scheduled
101	725	The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.	Not scheduled
102	731	The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans.	Version 2
103	739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 4
104	748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are	Version 4

Issue #	Paragraph #	Text	Phase[1]
		successful and backup failures are addressed, so that backups are available for future use.	
105	757	Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations.	VRF Filing(s)
106	759	Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.	VRF Filing(s)
107	767	The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors.	VRF Filing(s)