NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Draft 15th Meeting Executive Summary
Cyber Security Order 706 SDT — Project 2008-06

November 16, 2009 | 5:00 PM to 9 PM EDT
November 17, 2009 | 8:00 AM to 5 PM EDT
November 18, 2009 | 8:00 AM to 5 PM EDT
November 19, 2009 | 8:00 AM to 3 PM EDT

Orlando Utilities Commission, 6003 Pershing Ave.
Orlando Florida 32822

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

CSO706 SDT November 16-19, 2009 Meeting Summary Contents

Appendices

CSO706 SDT NOVEMBER 16-19, 2009 MEETING

EXECUTIVE SUMMARY

On Monday evening 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. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines.

Mr. Mix reminded the SDT of the FERC Order and 90-day response presented at the Kansas City meeting in October and provided an overview of the industry comments received the proposed revisions of CIP-002-2 through CIP-009-2, the Implementation Plan for Version 3 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, developed by the standard drafting team as part of Project 2009-21 Cyber Security Ninety-day Response. Mr. Mix noted that There were 29 sets of comments, including comments from more than 60 different people from approximately 40 companies representing 8 of the 10 Industry Segments.

The SDT reviewed, discussed and refined an initial strawman draft response document for CIP Version 3 prepared by Scott Mix for the 29 sets of comments received. At the end of Monday evening's meeting drafting assignments were reviewed. The SDT followed up on Tuesday morning and early afternoon and reviewed a refined document that included some new draft language for the consideration of comments document. The SDT reviewed a final draft with several revisions on Wednesday morning and unanimously adopted it for posting.

On Tuesday morning, Mr. Bucciero conducted a roll call of members and participants in the room and on the conference call and reviewed the need to comply with NERC's Antitrust Guidelines as he did on each of the following meeting days.

On Wednesday morning Scott Mix provided an Update on VSLs/VRFs noting that ballot had closed last Thursday with a high level of industry support. This would be approved by the NERC Board of Trustees and submitted to FERC. He noted the chair of the VSL/VRF SDT has volunteered to come in and give an update to the Team in January. In terms of the Version 2 VSL/VRF Mr. Mix indicated that there will have to be a correction for a technical error but that it looks like it will be approved which will close that group's work. The CSO706 SDT will be responsible for the VSLs/VRFs for Version 4. The SDT VSL/VRF chair will talk with the CSO706 SDT about their experience early next year to help us take on the task later in 2010.

SDT member discussed the updates on work related to the "smart grid" and its relation to the CIP development including the smart grid efforts and the need for coordinating this with the SDT's work.

Mr. Mix provided an update on the TFE process indicating that NERC is not expecting further actions by FERC – but will have to wait and see. He noted a compliance bulletin has been issued which directs industry to prepare for compliance – regions and NERC having discussions for a uniform system of compliance, should benefit those with coverage into different regions – have not seen a backlog of TFEs. The members discussed class based TFEs, mitigation plans, compliance schedules, and application to CAs and CCAs.

On Tuesday, facilitator Mr. Langton reviewed the workplan suggesting the SDT complete its initial draft of CIP-002-4 for posting by the conclusion of the December, 2009 meeting and launch the effort to develop the suite of controls (CIP 003-009) in early 2010. This will be a challenging parallel process with the SDT responding to industry comments and refining CIP 002-4 while simultaneously developing CIP 003-009. He noted that in January the SDT will review and agree on how best to organize to deliver on the milestones in the accelerated workplan.

At the end of the session on Tuesday afternoon, the SDT, at the request of NERC, engaged in a "blue sky" brainstorming session on ways to streamline the development process. The Team identified 36 suggestions in the following six categories: Changing ANSI Standards Procedures (3 options); Meeting Changes- Efficiency, Location, Tools (5 options); Commitment, Communication and Support (9 options); Team Structure (3 options); Substantive Changes in Approach/Scope to Standard Development (10 options); and More Talent and Expertise to Support SDT (6 options).

The Team agreed to engage in an exercise on Thursday to prioritize these options in terms of the highest priority and most helpful in facilitating the CIP standards development process. The results of the survey completed by 15 SDT members produced the following 5 options that received higher than a 4 rating on a 5-point scale *(from most helpful to don't do it):*

1. (4.46) Technical writer support (more writers like Scott Mix) (NERC) (11-5's & 4's and 2 -1's & 2's)
2. (4.43) Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc. (NERC in Coordination with SDT) (11-5's & 4's and 0 -1's & 2's)
3. (4.36) Make the best use of our time. Start meetings on time and get the technology operational early(SDT)(8-5's & 4's and 0 -1's & 2's)
4. (4.21) Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process. (NERC) (7-5's & 4's and 1 -1's & 2's)
5. (4.00) Engage technical writers (NERC) (8-5's & 4's and 3 -1's & 2's)

On Thursday morning, the Chair and Vice Chairs participated on behalf of the SDT in a conference call with Mike Assante and Gerry Adamski at NERC and Alan Moser the Vice Chair of the NERC Standards Committee to discuss NERC's guidance to the Team on the schedule the Team reviewed and revised at their Kansas meeting in October. The NERC representatives provided background in what is driving their schedule concerns noting in particular a perception from FERC and some on Capitol Hill that progress on Order 706 directives has been too slow which was underscored with the NERC survey back in the Spring. They noted that they believed that at least the CIP 002-4 (the asset categorization piece) needs to be filed with FERC by midyear and the CIP 003-009 by the end of the year. They offered commitment to providing the Team with whatever is need in terms of resources and communication with industry. The Team discussed the schedule and expressed concerns that: CIP 002-4 should not be watered down to fit today's CIP 003-009; that it might be difficult for the industry to adopt CIP 002-4 without seeing the controls in CIP 003-009; and the NERC conversation wasn't with the full team.

The Chair reviewed with the SDT the deliverables needed for posting in December, 2009 including: CIP-002-4 Requirements and measures; Sample controls (2-4 examples); Comment form with questions; Guidance document; Intro or cover letter; Related VSLs/VRFs: and Definitions.

John Lim provided an overview of Version 4 CIP 002 Strawman Draft Documents noting the current draft was still missing some definitions for the BES, generation and transmission subsystems and control centers. He noted that Jackie Collett and a sub-team (Scott Rosenberger, Gerry Freese, Jay Cribb) are tackling the definitions. He suggested that the critical assets guideline has started to create a definition that may serve as a starting point. Finally he pointed out that all of the generation assets in this draft has been moved from high to the medium level and that no unit by itself is considered high, but generation system could be in high. High also includes the major transmission facilities.

On Wednesday morning after reviewing and finalizing and adopting version 3 considerations document, the SDT broke into the following drafting groups for CIP 002-4: BES subsystem description/definition (led by Jackie Collett); Reliability functions definitions (led by John Varnell); Control Samples (Led by Keith Stouffer); and Guidance Document (led by Phil Huff). The facilitators noted that the SDT had to balance: getting it right; with getting enough consensus for acceptance; with getting it done in a timely manner. The SDT needs to optimize the three together.

Jackie Collett reported on the BES Subsystems Descriptions small group's results noting that they had a good start on a definition. John Varnell report that his group had developed 9 definitions for reliability functions and they had added definitions for each of the functions and included the examples which will be an attachment at end of CIP 002-4 standard and serve as a foundation for later sections.

Keith Stouffer noted that his group had developed two samples. He noted that the tables are designed to help the industry to understand the categorization process. The drafting group took two standards 009 and 006 to show how the categorization process might apply and their related requirements and asked the question: what is in the standard now is a "high" baseline. He suggested that even though we are adding categories, if you are low impact, there will be fewer requirements levied upon you.

Phil Huff noted that the Guidance Document group had found a way to simplify and the revised draft represented a major shift in name of simplicity. The proposal is to use the reliability functions for determining your BES cyber systems.

On Thursday, the drafting groups reported to the SDT. Keith Stouffer mentioned that in terms of the controls table format, the next big step to develop the information paragraph at the outset of each of the tables. Phil Huff noted that the Guidance Document would be developed further and circulated to the SDT in advance of the Little Rock meeting. The Chair noted she would circulate a draft of the "Comment Form". John Lim agreed to revise the CIP 002-4 draft for a preview in early December and then refine it and send it out to the SDT prior to the Little Rock meeting. Jackie Collett asked for time on the Little Rock agenda to go through a "walk through" of the CIP 002-4. She agreed to work with several SDT members to prepare materials for the walk through. NERC Staff (Maureen Long, Dave Taylor and Joel De Jesus) joined the SDT on Thursday morning and offered guidance in drafting the CIP 002-4.

The SDT Chair and Vice Chairs reviewed with the Team the updated agreed upon schedule for both the CSO 706 SDT Version 3 CIP and the Version 4 CIP 002 Process as follows:

CIP Version 3 Key Steps/Schedule

1. November 30, Monday *(after Thanksgiving)* Deadline for Votes and Industry Comments
2. December 2, Wednesday, CSO 706 SDT - Conference Call- finalize Response document to Industry Comments
3. December 3- 13, Recirculation Ballot
4. December 16, BoT Approval
5. December 29, 2009, FERC Filing

CIP 002-4 Key Steps/Schedule (October-December 2009)

1. December 7, 3:00-4:30 p.m. est. Previews of reviewed CIP 002 and related document drafts at a SDT conference call.
2. Other drafting groups will organize and schedule meetings prior to Little Rock.
3. The SDT will refine and circulate a revised strawman Draft by Monday, December 14, 2009 for review at the December 15-16 CSO706 SDT meeting in Little Rock
4. December 15-16 will refine, finalize and adopt draft CIP 002-4 for posting to the industry for informal comments.

The Chair reviewed the next steps including the schedule for the Version 3 response document and the CIP 002-4 effort. She thanked Rich Kinas for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 2:00 p.m. on November 19, 2009.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CSO706 SDT NOVEMBER 16-19, 2009 MEETING SUMMARY

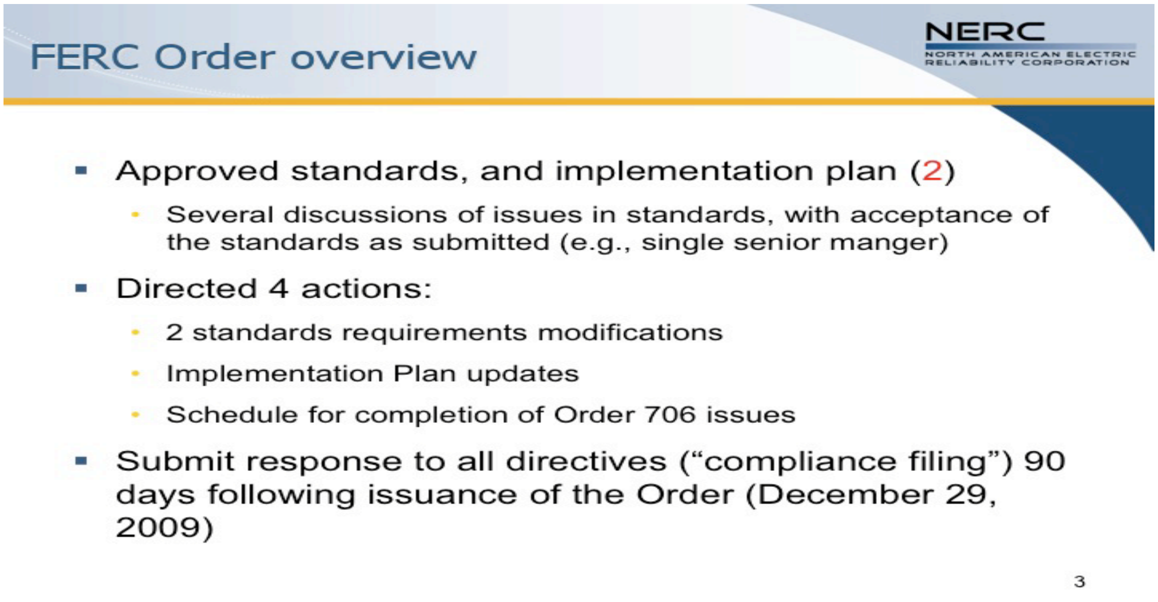
I. FERC ORDER ON CIP VERSION 2 AND VERSION 3 COMMENT RESPONSE DOCUMENT

A. Introduction

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

B. CIP Version 3 90-day Comment Response Document

Mr. Mix reminded the SDT of the FERC Order and 90-day response presented at the Kansas City meeting in October:



FERC Order overview

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Approved standards, and implementation plan (2)
  - Several discussions of issues in standards, with acceptance of the standards as submitted (e.g., single senior manger)
- Directed 4 actions:
  - 2 standards requirements modifications
  - Implementation Plan updates
  - Schedule for completion of Order 706 issues
- Submit response to all directives ("compliance filing") 90 days following issuance of the Order (December 29, 2009)

3

He provided an overview of the industry comments received the proposed revisions of CIP-002-2 through CIP-009-2, the Implementation Plan for Version 3 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, developed by the standard drafting team as part of Project 2009-21 Cyber Security Ninety-day Response. These standards were posted for a 30-day public comment period from October 13, 2009 through November 12, 2009. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form that included the following questions:

1. In its order approving CIP-002-2 through CIP-009-2, the Commission directed NERC to make changes to CIP-006-2 and CIP-008-2 as well as the implementation plan for newly identified critical cyber assets and file those changes within 90 days of the order. Do you agree that the SAR accurately addresses the scope of these directives? If not, please identify what you feel is missing in the SAR.
2. Do you agree that the proposed modifications to CIP-006-2, CIP-008-2, and the implementation plans meet the intent of the Commission's directives? If not, please identify what changes you feel are needed to meet the intent of these directives.
3. Do you have any additional comments associated with the proposed SAR for Project 2009-21: Cyber Security Ninety-day Response? If yes, please explain.
4. Do you have any additional comments associated with the proposed CIP-006-2, CIP-008-2, and the implementation plans? If yes, please explain.

Mr. Mix noted that There were 29 sets of comments, including comments from more than 60 different people from approximately 40 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

The SDT reviewed, discussed and refined an initial strawman draft response document for CIP Version 3 prepared by Scott Mix for the 29 sets of comments received. At the end of Monday evening's meeting drafting assignments were reviewed. The SDT followed up on Tuesday morning and early afternoon and reviewed a refined document that included some new draft language for the consideration of comments document. The SDT reviewed a final draft with several revisions on Wednesday morning and unanimously adopted it for posting as show on the following pages:
http://www.nerc.com/docs/standards/sar/C-of-C_Cyber_90
day_Response_Initial_Ballot_2009Dec3.pdf

A. 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*).

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

B. Updates

VSLs/VFRs. On Wednesday morning Scott Mix provided an Update on VSLs/VRFs noting that ballot had closed last Thursday with a high level of industry support. This would be approved by the NERC Board of Trustees and submitted to FERC. He noted the chair of the VSL/VRF SDT has volunteered to come in and give an update to the Team in January.

In terms of the Version 2 VSL/VRF Mr. Mix indicated that there will have to be a correction for a technical error but that it looks like it will be approved which will close that group's work. The CSO706 SDT will be responsible for the VSLs/VRFs for Version 4. The SDT VSL/VRF chair will talk with the CSO706 SDT about their experience early next year to help us take on the task later in 2010.

Other Cyber Security Initaitives. SDT member discussed the updates on work related to the "smart grid" and its relation to the CIP development.

SDT Comments on Related Cyber Security Initiatives

- Don't hear us talking much about smart grid or smart grid people talking much about the CIP standards – seem to have a gap in communication
- NERC standards only apply to the BES assets – not small production – smart grid is looking at everything from production, transmission all the way into the home –
- NIST is getting lots of pressure to roll things out.
- Who is supposed to be making the link? There is a group that is supposed to coordinate security across all the groups. But key issues haven't been raised to date such as: do we really want a system that is fully inter-operative? Do we want millions of smart meters running through the same system as our control systems? If it works really well in AMI how do you make sure it is good for transmission or is complimentary – also note it is another security system to be aware of and prepared for.
- A Wisconsin study commissioned by FERC was briefly discussed.

Technical Feasibility Exceptions. Mr. Mix provided an update on the TFE process indicating that NERC is not expecting further actions by FERC – but will have to wait and see. He noted a compliance bulletin has been issued which directs industry to prepare for compliance – regions and NERC having discussions for a uniform system of compliance, should benefit those with coverage into different regions – have not seen a backlog of TFEs

Member Comments on TFE Update

- What is going on with class based TFEs?
- Personal view – list is an after the fact addition to the list once we see what is out there rather than trying to come up with a complete omniscient list to start with
- Mitigation plans? Personal opinion – do not give examples because too many will rely on example as to how to comply, rather leave it up to individuals to determine what to do with TFEs initially
- Do not see class will give companies much help in defining mitigating measures – not buy you much time
- Why January cut off if you can retroactively identify and add to the list?
- Does the device you are requesting TFE on have to be a CA or CCA? May not identify if there is disagreement within an organization or may identify only to cover potential.
- Standards only apply to CCAs. Sounds like you are creating a significant workload for approval for something you will not be held accountable for. No harm waiting until it is on the CCA list.

A. WORKPLAN REVIEW AND STREAMLINING THE CIP DEVELOPMENT PROCESS

A. Workplan Review

Mr. Langton reviewed the workplan suggesting the SDT complete its initial draft of CIP-002-4 for posting by the conclusion of the December, 2009 meeting and launch the effort to develop the suite of controls (CIP 003-009) in early 2010. This will be a challenging parallel process with the SDT responding to industry comments and refining CIP 002-4 while simultaneously developing CIP 003-009. He noted that in January the SDT will review and agree on how best to organize to deliver on the milestones in the accelerated workplan.

B. Considerations in Streamlining the CIP Development Process

At the end of the session on Tuesday afternoon, the SDT, at the request of NERC, engaged in a “blue sky” brainstorming session on ways to streamline the development process. The Team identified 36 suggestions in the following six categories:

A. CHANGING ANSI STANDARDS PROCEDURES (3 options)
B. MEETING CHANGES- EFFICIENCY, LOCATION, TOOLS (5 options)
C. COMMITMENT, COMMUNICATION AND SUPPORT (9 options)
D. TEAM STRUCTURE (3 options)
E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT (10 options)
F. MORE TALENT AND EXPERTISE TO SUPPORT SDT (6 options)

The Team agreed to engage in an exercise on Thursday to prioritize these options in terms of the highest priority and most helpful in facilitating the CIP standards development process. The results of the survey (See Appendix # 6) completed by 15 SDT members produced the following 5 options that received higher than a 4 rating on a 5-point scale (from most helpful to don't do it):

1. **(4.46) Technical writer support (more writers like Scott Mix)** ***(NERC) (11-5's & 4's and 2 -1's & 2's)***
2. **(4.43) Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc.** *(NERC in Coordination with SDT)* ***(11-5's & 4's and 0 -1's & 2's)***
3. **(4.36) Make the best use of our time. Start meetings on time and get the technology operational early***(SDT)****(8-5's & 4's and 0 -1's & 2's)***
4. **(4.21) Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process.** ***(NERC) (7-5's & 4's and 1 -1's & 2's)***
5. **(4.00) Engage technical writers** ***(NERC (8-5's & 4's and 3 -1's & 2's)***

In terms of possible substantive changes to the SDT approach or scope the ranked the following 10 strategies on the 5-point scale:

E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
3.62	Refocus on security issues and less on compliance *(SDT)*	**8**	**3**
3.54	Remove penalty base requirements (you get what you measure) *(NERC,* *FERC, Congress)*	**6**	**4**
3.46	Simplify the approach and strategy to the standards to reduce com *(SDT)*	**7**	**3**
3.08	Adapt 800-82 (targeted for industrial control systems) *(NERC & S*	**3**	**7**
2.92	Adopt 800-53 Rev 3 for control centers and data centers *(NERC & SDT)*	**4**	**6**
2.92	Review Order 706 and remove items included that should be give	**4**	**5**

	another group, challenged or deferred. *(NERC & SDT)*		
2.46	Throw in with CSCTG from NIST *(NERC)*	**2**	**8**
2.38	Go back to the 'original, original' standards for cyber security as a basis for the new CIP (see NERC Website archive) *(SDT)*	**2**	**7**
2.08	Skip BES Mapping and install minimum security controls for all a after establishing clear cut agreed upon objectives on what we are securing. *(SDT)*	**2**	**10**
1.85	Abandon the NIST based approach and improve existing standards framework. *(SDT)*	**0**	**13**

On Thursday morning, the Chair and Vice Chairs participated in a conference call with Mike Assante and Gerry Adamski at NERC and Alan Moser the Vice Chair of the NERC Standards Committee to discuss NERC's guidance to the Team on the schedule the Team reviewed and revised at their Kansas meeting in October. The NERC representative provided background in what is driving their schedule concerns noting in particular a perception from FERC and some on Capitol Hill that progress on Order 706 directives has been too slow which was underscored with the NERC survey back in the Spring. They noted that they believed that at least the CIP 002-4 (the asset categorization piece) needs to be filed with FERC by midyear and the CIP 003-009 by the end of the year. They offered commitment to providing the Team with whatever is need in terms of resources and communication with industry.

SDT Member Comments on the Schedule

- NERC wants to know what we need to do the job. Getting the asset categorization issue fixed and filed.
- Exercise with language in CIP requirements- SDT does a cut these existing requirements apply to H/M/L.
- Impact level piece of CIP out there. Could be a transition point and is familiar for industry.
- Addressing directives and FERC order and problems identified in CIP requirements.
- May need a Version 5 or more.
- NERC Acknowledged the concept paper and suggested the Team is on the right path.
- Nervous about writing the new 002 and apply 3-9 beneath it. 3-9 as they are now only apply to the high.
- Don't water down the new 2 to fit with the 3-9 today. Get 002 right and then tweak 003-009.
- Concern of pushing 002 to ballot ahead of 003-009?
- How to handle the critical/non critical.

- If we do this on version 2- don't leave pieces in that will cause problems in just changing CIP 002.
- Not just changing categorization of only BES assets. Could be dangers down this path.
- We have to finish this job.
- How is the industry going to feel about being thrown a different set of requirements- then another change.
- Will the industry have to do anything with the controls? Especially mentioned an implementation plan.
- This would be expected to be done?
- If go H/M/L on existing requirements? Industry will have to apply to more stuff. But the plan is to have all of the CIPs done in 2010.
- June 2010- CIP 002 balloted. Current requirements should be at least applicable to all the highs.
- Will entities identify additional high assets that were not critical?
- The implementation plan should address how much time you give the entities to apply the controls to meet the requirements for the newly identified high impact facilities.
- Medium and low? Take current requirements and determine which are applicable to medium resulting in another implementation schedule.
- Main concern is to put something out there to push industry to stop "gaming" the system. You are going apply 3-9 to the high level categories at a minimum and then file your TFEs
- For part of the Order 706 directives, we are showing progress.
- Interim measures may not a good value.
- 2 issues on urgency raised by NERC- perceived deficiencies. FERC and Congress believe there are a lot of facilities that should be critical but are not. Second the all or nothing approach of the current standards.
- Our concept paper laid out the proposition that everything needs some level of protection- i.e. "all in."
- Concerned that NERC didn't open up this discussion to the whole team. Would have been less disruptive and more efficient.
- Another way: going with formal comments- implementation plan change.
- Going to ballot on Friday for the implementation plan. We are about to ballot something that will have impact which will change all that. This comes along with V2 as part packet.

- June for just CIP 002? Another 7 months?
- This is not a surprise. 6 months/ another 6 months. We have ignored the growing concerns and this has happened. Doesn't see a problem with 3-9. We can do a better job.
- New CIP 002 would introduce new categories. Connectivity issue was to be addressed later by controls. i.d. by CAs without CCAs. Big count.
- Would the existing 3-9 given H/M/L on each requirements meet the Order 706 requirements? Probably not. The industry may not vote yes if you don't know what you are going to have to do in 003-009.
- If we are going to get this done, the SDT needs NERC at every meeting with their attention solely on this meeting. They need to answer questions at the moment they come up so we will need someone with authority and expertise.
- I am not surprised about time crunch. Direction doesn't surprise. 002 doesn't surprise. What is the proposal for 003-009 requirements?
- Is the expectation of industry approval of 002 without knowing exactly what this means. What do I do now? This was something to do with the 3 lists.
- We should seek to get a fairly solid CIP 002 in December and stick with that.
- Likes this approach of providing some relief of participating team members and their organization from CIP audit schedule.
- Congressman Langevin asked Jon Stanford about progress being made by the SDT. Congress recognizes the hard work and challenges we have. Mr. Stanford asked what he should bring back to the Team from him. He said to tell the Team to continue the hard work and try to work towards a NIST like model with impact levels for assets. Our current path could receive a lot of support from congressional side. We know that if we don't change the standards, there will be legislation. There are at least several draft bills pending. Need to think about our priorities for cyber security and no so much about the ballot body.

IV. CIP 002 VERSION 4 STRAWMAN

A. Introduction

The Chair reviewed with the SDT the deliverables needed for posting in December, 2009 including: CIP-002-4 Requirements and measures; Sample controls (2-4 examples); Comment form with questions; Guidance document; Intro or cover letter; Related VSLs/VRFs: and Definitions

B. Overview of CIP 002-4 Strawman

John Lim provided an overview of Version 4 CIP 002 Strawman Draft Documents noting the current draft was still missing some definitions for the BES, generation and transmission subsystems and control centers. He noted that Jackie Collett and a sub-team (Scott Rosenberger, Gerry Freese, Jay Cribb) are tackling the definitions. He suggested that the critical assets guideline has started to create a definition that may serve as a starting point. Finally he pointed out that all of the generation assets in this draft has been moved from high to the medium level and that no unit by itself is considered high, but generation system could be in high. High also includes the major transmission facilities.

SDT Comments on Strawman Draft

- Some others have already set markers as to what they think is high – do we need to socialize those with ours? What happens if our list is less? Is that politically acceptable?
- We may eventually be told what to include and need to focus on the controls.
- Still having trouble understanding if intent of step 2 is to categorize by impact and step 3 is to assess impact on the BES – where are we in syncing these pieces?
- Two separate assessments, but have to do both assessments to understand the related impact on each other.
- R2 feeds into R3 – not completely separate assessments.
- Want to be sure we keep going down the path we are headed regardless of whether or not we think they may come in and take it away from us
- Want to be sure we produce a polished product the industry can understand and use
- How the two pieces come together may be addressed in the Guidance document.
- Uncertain whether we need to include a reliability function assessment – brought it down from three to two level system of high/low
- The current strawman takes a low water mark approach rather than the high water mark approach.
- Detection starts with who “owns and operate” – should it be “owns or operates it”? Big difference
- Like the definition of high and low but still begs question of “none”
- “None” may falls out of the definition of BES cyber system
- In case of a generator – if I have just one and my role ends there, do I have to make an assessment? Can they get the information they need from the generation system to make the assessment?

- You can get pricing data but not much else
- Reviewed tables/matrix in response to “none”
- Reliability coordinators can decide this.
- R3.2 in the matrix – from “optics” perspective difficult to explain why it drops from high to low
- Are assets being assigned to the BES system or the subsystems?
- It is not the concept but the wording that causes confusion. Change to “assigning the reliability impact to the BES cyber system that supports the subsystem” (wording from Jackie Collett)
- R2.4.2 vs. R4: separate requirement in each or just one time?
- Problem is with initial list – explicitly calls each out to avoid question of whether I must have a list before compliance assessment.
- Senior manager signs off on original and annual.
- Matrix – function impact correlates to cyber systems – may need to adjust the high BES impact and function impact from low to medium.
- Just because there is connectivity doesn’t mean something will go through.
- Concerned about the level of complexity we are creating – more words give more opportunity to vector off course.
- There are a lot more words but a simpler system to use than what we have currently – we will probably make mistakes, but also progress.
- We were told last week by NERC not to use the measures in an assessment. Measures are included in the requirements here for that reason.
- In our recent NERC audit they did not use measures, only looked at requirements
- Intent is to include it in an appendix to the standard.
- We need examples to illustrate the tables –
- We will have descriptions of the functions in the next day or so as well as the definitions.
- Keep in mind the comment form questions too
- Existing single control example shows little gradation
- Hope to have a second example with more gradation drafted tomorrow (Keith, Bill and Joe will work on)

C. CIP 002-4 Small Group Discussions

On Wednesday morning after reviewing and finalizing and adopting version 3 considerations document, the facilitators reviewed the proposal for the SDT breaking into the following drafting groups for CIP 002-4: BES subsystem description/definition (led by Jackie Collett); Reliability functions definitions (led by John Varnell); Control Samples (Led by Keith Stouffer); and Guidance Document (led by Phil Huff).

SDT Comments on the Proposal:

- What are we doing with brainstormed list of ideas? The Chair noted she contacted Mike Assante by email last night and he agreed to call in later today to discuss then full group can discuss ways to accelerate the work plan.
- I have a concern that we spend time today and tomorrow going down the wrong way if we are going to entertain a new direction?
- We have made a commitment to NERC, industry and congress to get the CIP 002 review document out in December 2009 and we are close. If the SDT revisits our decisions it may derail the progress we have made on the December deliverable.
- Would be a disservice to put something out that will not work or is not understood.
- If put something out it has to be credible – good start but not enough time to vet decisions we are making – recommend starting a small subgroup to work in parallel to look at modifying current CIP standard to see how much of the FERC order can be incorporated – it stands the best chance of getting approval by the June time frame.
- When we put the concept paper out in July, we thought we would get more push back – it was more accepted than expected – commitment as a group to take a certain approach and have invested a year – have not heard negative comment from the industry for the approach we are taking – underestimating it would take to modify current standard – just as much effort as the approach we are taking – rehashing the same issue over again would be a step backward and impede us from focusing on our objectives and charge.
- The facilitator noted that the SDT is balancing three values:
  - 1. Getting it right;
  - 2. Getting enough consensus for acceptance;
  - 3. Getting it done in a timely manner. The SDT needs to optimize the three together – yesterday was an opportunity to put ideas on table, need to hear back from NERC before we discuss the issues further.
- Going back into 706? One big issue was criteria for selection, could be a show stopper if Regions refuse to do it – looking at order is a good idea but on this point could be arguing for a year without resolution.
- Modifying current CIP 2 would not be derailed by consideration of external reviews

- Issue is not about philosophy but rather one of resources and liability. Regions are very concerned.
- Lack of industry response may not be acceptance – could be a lack of understanding or commitment to engage until they get a final version. This needs to be crisper more easily understood --complexity is a problem.
- NERC has many balls in the air for industry to consider and respond to at the same time

On Wednesday the facilitators reviewed the proposal for the SDT breaking into the following drafting groups for CIP 002-4:

1. BES subsystem description/definition (Jackie Collett, Scott Rosenberger, Gerry Freese)
2. Reliability functions definitions (John Varnell, Rick Kinas, John Lim, Doug Johnson)
3. Control Samples (Keith Stouffer, Bill Winters, Jeri Brewer Domingo, John Stanford, Sharon Edwards and Jim Breton)
4. Guidance Document (Phil Huff, Dave Revill and Rob Antonishen) – needs help to review for accuracy of process, and the generation, transmission and control

Following small group meetings, the leaders of each group presented a report to the full SDT.

1. **BES Subsystems Descriptions**

Jackie Collett reported on the small group's results noting that they had a good start on a definition. The group is looking at basic building blocks for each.

SDT Member Comments and Guidance

- Generation- "Big Iron" side. Cyber system treated as a subsystem? Yes.
- BES Subsystem not defined as a single thing. Combinations of units that create an impact. Words intended to drive towards identifying combinations.
- Transmission subsystems.
- Control Centers- CIPSE critical asset guideline.
- How did you determine how a subsystem? Is there a common BES transmission bus(s) connecting generation units?
- Collection of units supported by a shared cyber system.
- From BES side and from the Cyber side- separated in documents.

2. **Reliability Functions**

John Varnell noted that they had developed 9 definitions for reliability functions and they had added definitions for each of the functions and included the examples. This will be an attachment at end of CIP 002-4 standard and serve as a foundation for later sections

SDT Member Comments and Guidance

- Is there anything in reliability in functions not included in BES mapping functions?

3. Control Samples

Keith Stouffer noted that his group had "kicked some CIP ass" and described two samples they have developed. He noted that the table are designed to help the industry to understand the categorization process. The drafting group took two standards 009 and 006 to show how the categorization process might apply and their related requirements and asked the question: what is in the standard now is a "high" baseline. Pare back for medium and low systems. Should note that even though we are adding categories, if you are low impact, there will be fewer requirements levied upon you. They will put this into new standard format and displaying same content in table or requirement formats. Stuck to low moderate and high. Not ready yet.

SDT Member comments

- Assumption is current CIP are all high? Because they apply to critical assets?
- Careful we don't get boxed in.
- Make clear that this is only showing an existing standard not what the 009-4 standard will look like.
- Took declaratives from FERC order? E.g. Firewalls from multiple vendors.
- Concerned with adding complexity by getting into the particulars/standards at this point.
- Give a before and after example. Mapping before and after. Access control requirement.
- How much complexity are in these examples?
- We told industry that we have been building upon work already being done. Shows a transition to a future- where you will have impact levels. Ability to target resources.
- This is not time to introduce something complicated- don't use the access control requirement.
- How does this relates to currently existing to show where we are heading? We need to be clear that requirements will be changes, moved around, added as we add a full suite of standards.
- Unlike other attachments, this will be an addition separate from the standard.
- This connects the dots to work going on now to future proposals.
- Everyone now doing the high and that these things will get simpler?

- Assets under consideration will be expanded to apply security protection- but not as onerous as the current critical assets now.
- Assume 10% classified as critical. Applying all controls to that 10%. Other 90% have to do something, but it will be less.
- Is this a roadmap as to how to do nothing?
- Reservations- this looks like the medium and lows don't have to do much. Careful with chart.
- Problem is with the presentation- summary at beginning and format.
- 800-53 families- similar- something required if low moderate high. Others little required is a low.

4. Guidance Document

Phil Huff noted that the group had found a way to simplify and the revised draft represented a major shift in name of simplicity. The group understood that the reliability function impact married together in the "hook up table" is confusing. If the team doesn't understand, won't communicate well in the industry. The proposal is to use the reliability functions for determining your BES cyber systems. Then back to impact criteria for BES system. No mapping will be needed. Simplifies significantly and reduces complexity.

SDT Member comments

- Does this negate everything we have done? No, this is not a major shift- build on reliability functions.
- Single row look up table.
- Same scoping exercise- Take BES cyber systems only in look up table. We are here for BES.
- Starting either with cyber or BES subsystems is valid in scoping your cyber systems.
- Once you scope your cyber systems. You inherit the impact level of whatever the BES subsystem supporting happens to be.
- H/M/L- if you have a cyber system supporting BES subsystem- cyber subsystem inherits.
- An entity has to do both parts. Unless both parts are done won't be right. Who merges the two pieces. IT more capable of merging the two? Can't do one and make assumptions about the other.
- This is not a IT/engineering fight. Still have to look at reach of cyber system.
- Will this be doomed for failure? Assume IT reach of the system.   Won't be Bulk Power people. They will make assumptions that will be wrong.

- Energy management system (e.g. servers, routers, firewalls), before that applications data, in terms of IT people- individual components. They identify all components. Need to go to applications and see what the functions are. We assess the impact of the functions. Then we map. We are done. Box now becomes the AGC mapping. Automatically rolls to the BES impact mapping. IT and Operations- automatically maps to the function. IT not making an objective judgment.
- The problem is we can’t say how this all is going to work.
- I can give these criteria to our people and get the work done.
- Operations people in the field. What are the important things we have to do. Started with the applications. What do they talk with etc. They came up with where the data stored. Understood reach of critical reliability functions. You know the reach of the app and where the data is flowing to, you can determine criticality.
- We are here to do cyber security- not BES. What are we trying to secure?
- We need a matrix- BES and cyber piece. Started with functions. What does it take to do on cyber side. Take BES pieces.
- We are not throwing out matrix, rather we have reduced it to single row. If cyber subsystem has impact to the BES, this is based on the BES impact.
- Started with functions, applications.
- Start with the “terminals”- in the field-? Need the feeds from the field- need to turn on/ off.
- Understating the stuff out there? Looking at BES in very narrow areas. Control centers are easy.
- It is a 1 by 3. We need to simply the process
- 3 by 3. Why don’t we need it anymore?
- Focus on what are you performing an impact assessment on? Cyber Impacts reliability functions. Criteria for reliability.
- Cyber asset that affects multiple functions.
- We are still trying to map to subsystems- will try to show this visually.
- If you start with BES items, you may not have to look at so many cyber assets.
- Data flow modeling? Need to use this as a tool to help with determining what is critical. Enterprise architecture modeling tools would have value. E.g. have a relay as a cyber device. Low medium high for that device. It’s the BES thing that matters?
- Are we confusing connectivity and communication vs. the focus on the device?
- BES high-impact to BES reliability function. First identify the reliability functions.

- Have a list of cyber systems- this may be a big assumption that is not incorrect.
- The SDT should treat as an ongoing process which will be designed to reduce that gap as you go forward. It is a change management strategy.
- Is that path too risky?
- In terms of the 3-3 game. When you do it. Fill in with examples.
- How to tell the difference between the rows and the columns?
- Hypothetical- switchyard is a low medium high. Cyber assets within switchyard. L/M/H. High= loss or compromise would immediately cause. What is the function- of switch yard. 500 KV line. Operation of a single break?
- Look at high impacts to the BES function. Lost, compromised. What about connectivity?
- Is this dealt with by controls?
- If no on connectivity, makes it lower.
- E.g. two identical physical devices one is connected the other is not. Have a different cyber impact?
- Why are you dealing with physical?
- If not connected, are they out?
- Looking at cyber asset- what's the cyber impact of this connected relay. The one not connected fall off the list.
- Separating BES analysis and a cyber analysis-
- Cyber perspective the impact may be higher.
- Impact analysis is separate from the cyber assessment.
- Is cyber about connectivity? Wouldn't have physical requirements.
- Impact to a function- walk into yard.
- Game is not helping very much.
- Struggling with a way to explain to the industry to show how we fit together.
- If we can't express it. Modify.
- When I say connectivity, it is a difference- but it is discounted by others.
- Communication and impact- Sweitzer relay on a line without connectivity. I can trip that line. If the relay has connectivity- I could get to it and fake it out. Can factor into a bigger impact. Connectivity adds another/extra layers of potential impacts that has to be factored in.

- Relay engineers- “Aurora” thing- if you get into a relays set low or high. Micro processor. BES impact with a non processor.
- Withdrawn game. Raised point- 2 different interpretations about what impact is. Difference between impact and risk. “Impact assessment” has to include potential risk or not? Need to determine this.
- This is not designed to for physical security. Threat exists of a terrorist states controlling from a remote. Connectivity is the key /core to this threat.
- Appreciates connectivity- how do you define the cyber system? Framework was about systems in a management ways including interconnection component. Define the impacts to the function. Examine what risks are at play whether interconnected or not. Some protections are physical. Look at procedural controls. Impact assessment vs. risk analysis—
- Are we talking about “systems” in an appropriate way?
- Someone gets into cyber relay and changes setting, Control center would not know. Can happen on any device in that substation.
- We should consider the MRC (Jerry Cauley) results based performance methodology. Would be helpful to understand what he’s looking for.
- The performance methodology has no official standing as yet. Won’t have in front of Standards- committee or this team by the time we finish our work.

5. CIP 002-4 Revisions

John Lim and Phil Huff presented revisions to the CIP 002-4 strawman.

SDT Comments on CIP 002-4

- Removed “senior leadership”- not BES impact categorization issue.
- If standards not viewed as a complete set. Audits 1 at a time. Must have senior manager sign off.
- Senior manager sign off in every standard?
- Consider a standard that everyone complies with that deals with governance issue. Then move into technical controls. Clear focus on soft issues. XX vs. 002.
- This should be explained in the cover letter that the Team is soliciting comments on technical area, while organization of standards has yet to be determined.
- R2: each BES subsystem associated with. Take the system high. E.g. associated with 1 BES, same as today. If you have multiple, take the highest category of those.

- Sub-requirements? VRF issue made. Break out 1,2,3. These are listed. May be clearer to see.
- If sub requirements, must be clearly written for future audits. Numbers do each.
- R3 redone. Combined R4 with R3.
- R1.4.2 eliminate-
- R1. R2 talks about BES cyber system. "For each"- need to identify and list.
- R1- copy and place categorizing list.
- Have to keep in mind how NERC audits- reported on a requirement level not sub-requirement level.
- Take requirement numbers off- bullets or options?
- Have to be numbered apply the "following criteria," not requirements.
- Writing of violations based on how writing the VSL? No. Only looked at once violation confirmed, what is the sanction or penalty.
- Are these standards for compliance?
- If posting like this? Don't want to accept but have to. But it is wrong.
- Are these criteria? Go through each one to apply criteria applicable to them? That is the way it is written.
- Only Rs will be in front of major requirements. Not requirements but under numbered lists. A violation of one thing way down, is a violation of the requirement?
- Each of the sub-requirements become requirements?
- A true violation is you didn't do the mapping, vs. 1 of the 16 things.
- Double jeopardy- single instance leading to a violation of 2 requirements.
- This could be tighter with fewer words. Reduce to a phrase. Considerations that should go into analysis. If you don't consider, maybe should be dinged. This is how to set up mappings- these are filters not requirements.
- Need to map and follow through with the mapping- in Version 2- "and implement"
- R1- is requirement. Rest of list is numbered list containing criteria in order to do the mapping and assign levels.
- Audit question- and fine requirements.
- This has the applicability right in the front.
- New template? E.g. VRF and VSL at R. 1.1.1 and each one.
- Remove the R- and you are in violation-

- One option would be to make R1-“identify and categorize impact levels”, apply criteria in an appendix to identify the impact levels. If in an appendix not mandatory.
- Does this leave us where we are now in terms of making up your own?
- Remove R1 as a statement and have instead an “Introduction.”
- Intro paragraph are outside of a requirement. Template doesn’t have a provision for introduction on a requirement lists.
- SDT needs to work within the boundaries.
- Make each sub/sub a requirement on its own? Each has to reference the requirement or category.
- Same amount of work you have to do.
- Need to level set – reframe the standards within the CIP structure. Look at this approach to categorization. Making everything a requirement? Have to do or deliver something. Requirement is to provide a process. Deliverable under R1- sub-requirements. If we do this, really a strange number of standards.
- Post something as a draft standard- or we post another concept paper that looks like a draft standard but doesn’t meet the format. More important to get a revised concept out to industry?
- Conceptually how you do categorization, this is what you do with this when you get it done.
- Revised detailed concept that will lead to a standard. Make it an outline.
- Have to worry about these things as doing process. Going to miss if we don’t.
- Support this approach.
- What of the discussion- BES subsystems not yet in?
- We will call this a working draft- post- of the mapping and categorization of BES cyber systems. Put something out that is close to a standard format. Putting out another concept paper won’t generate industry comments and input.
- Put this out- this is as far as we could get. How does this help us look at this in the future?
- NERC format- we need editors in the room. We are guessing at what they want. Dave Taylor. Maureen need to be at our next meeting.
- Commitment to draft standards in December. Problems with putting out in this format. Not a bad thing. Makes more apparent problems with current template that NERC has. Hard to explain to outsiders if we are doing a “concept”.
- The SDT needs to meet expectations for a standard. Don’t call a concept, instead call it a preliminary draft.

- The SDT has to agree on the concept of what we want people doing. Need to make it through- get the flow right- worry about the formatting later. We don't yet have the flow.
- Walk through the process and see if there is consensus.
- Scoping BES cyber system can be done from either direction- should come up with the same cyber systems.
- R2- "as determined in R1
- R2- any BES cyber system associated with any BES subsystems. If you go back to definition, some things are not BES cyber systems (e.g. revenue metering device, thermal data logger in generation system). Ascertaining a BES cyber system. Be clear- rewrite R1 as R2.
- Say it all over again just to be clear?
- Good with BES cyber system. But problems with Cyber system: "disposition of information"?
- Requirement – identify all your BES cyber system.
- We need to go through this from top to bottom.
- Use the tables as a starting point.
- Maureen Long and Joel De Jesus from NERC can help the SDT.
- NERC is trying to minimize the use of sub-requirements.
- Requirement a separate piece of work with some reliability benefit by itself. Removed R from sub requirements. Refer to as parts. If subject to liability itself.
- If a sub-requirement is embedded within a requirement- it will be treated and audits as a violation.

6. Summary of Discussion Points with NERC Staff

NERC Staff (Maureen Long, Dave Taylor and Joel De Jesus) joined the SDT on Thursday morning and offered the following guidance to the SDT:

1. Define in the Glossary: High Impact; Medium Impact; and Low Impact.
2. Remove the sub/sub requirements (R1.1.1., R1.1.2., R1.2.3, R1.2.4. etc.) from the draft standard and put them into a separate numbered list attachment document.
3. State in the attachment document that the Responsible Entity (TO, GO, BA, etc) has to comply with only the applicable items, i.e., TO does not have to include generation if it does not apply. They did not think this distinction of what items applied to TO or GO only was clear using the currently proposed draft standard format which was displayed on the Webex they were looking at.
4. Add to the main requirement what the impact is to reliability. Maureen stated that under

the new NERC template each requirement is to include how it contributes to reliability.

5. Use the existing latitude available in establishing violation severity levels (VSL's). Consider using percentages ,i.e.:
   - (Entity missed either <10% of items (or perhaps 4 items) = low,
   - Entity missed >10% but < 25% = Medium, etc.)
6. If the proposed standard remains in the format that is current proposed, as shown on the Webex, then any missed item will result in a finding of non-compliance by the auditor. As an example of how severe this could be, in the current draft standard format, auditing of a TO entity who did not have generation listed in their R1 analysis would result in a finding of non-compliance sent to compliance staff for further investigation.

V. NEXT STEPS

The SDT Chair and Vice Chairs reviewed with the Team the updated agreed upon schedule for both the CSO 706 SDT Version 3 CIP and the Version 4 CIP 002 Process as follows:

CIP Version 3 Key Steps/Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 SDT Conference Call- Review of Industry Comments and Response**
3. **November 16, CSO 706 SDT Meeting in Orlando, Monday, 5:00 p.m.- through dinner- Response Document to Industry Comments**
4. **November 17**, Tuesday, CSO 706 SDT Meeting, Orlando, Complete and Adopt Response Document to Industry Comments
5. **November 20**, Wednesday, Post Response Document and Initiate Ballot
6. **November 30**, Monday *(after Thanksgiving)* Deadline for Votes and Industry Comments
7. **December 2, Wednesday, CSO 706 SDT - Conference Call- finalize Response document to Industry Comments**
8. **December 3- 13,** Recirculation Ballot
9. **December 16,** BoT Approval
10. **December 29, 2009,** FERC Filing

CIP 002-4 Key Steps/Schedule (October-December 2009)

1. **November 1:** Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP 002 Subgroups will form the CIP 002 Strawman Drafting Group (SDG).
2. **November 1:** All CIP 002 "meta groups" and subgroups will forward to the Strawman Drafting Group their standards text drafts including any guidance language**.**
3. Joe Doetzl will coordinate the work of the Controls Drafting Group (CDG) members: Jim Brenton, Keith Stouffer, Bill Winters, Jon Stanford. They will produce several recommended sample controls to illustrate high/medium/low concepts in CIP 002 as well as recommendations on whether the SDT should request guidance from the

Standards Committee on referencing a 'catalogue of security requirements', for circulation to the SDT **by Friday, November 13, 2009**

4. The SDG will prepare a strawman draft by **November 13, 2009** for review by the SDT in advance of November 16-19, 2009 SDT meeting
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and determine at the conclusion of the meeting if the SDT will continue to aim for the December 16th adoption of CIP 002 draft for posting for industry comment
6. **December 7, 3:00-4:30 p.m. est**. Previews of reviewed CIP 002 and related document drafts at a SDT conference call.
7. The SDT will refine and circulate a revised strawman Draft by Monday, December 14, 2009 for review at the **December 15-16** CSO706 SDT meeting in Little Rock
8. **December 15-16** will refine, finalize and adopt draft CIP 002-4 for posting to the industry for informal comments.

Keith Stouffer mentioned that in terms of the table format the next big step to develop the information paragraph at the outset of each of the tables. Phil Huff noted that the guidance document would be developed further and circulated to the SDT in advance of the Little Rock meeting. The Chair noted she would circulate a draft of the "comment form" and cover letter. Jackie Collett asked for time on the Little Rock agenda to go through a "walk through" of the CIP 002-4. She agreed to work with several SDT members to prepare materials for the walk through.

The Chair reviewed the next steps including the schedule for the Version 3 response document and the CIP 002-4 effort. She thanked Rich Kinas for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 2:45 p.m. on November 19, 2009.

Appendix # 1— Meeting Agenda

NERC SDT Order 706 November 16-19, 2009 Meeting Agenda Packet

Project 2008-06 Cyber Security Order 706 SDT
Draft 16th Meeting Agenda
November 16, 2009, Monday - 5 PM to 9 PM EST
November 17, 2009, Tuesday - 8 AM to 5 PM EST
November 18, 2009, Wednesday - 8 AM to 5 PM EST
November 19, 2009, Thursday - 8 AM to 3 PM EST
Orlando Utilities Commission, 6003 Pershing Ave.
Orlando, Florida 32822

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Group Meetings May Not Have Access to Telephones and

Proposed Meeting Objectives/Outcomes

- Welcome new members and outline SDT leadership transition
- Review, Discuss and Adopt SDT Response Document to Industry Comments on CIP Version 3
- Review the CIP 002-4 and CIP 002-009-4 workplan going forward
- Receive updates on TFE, VSL/VRF and related cyber security efforts
- Review CIP 002-4 Key Issues and Provide Guidance to Documents Drafting Groups
- Convene CIP 002-4 Document Drafting Groups
- Review and refine a draft CIP 002-4 strawman and related documents
- Agree on next steps and assignments

Draft Agenda

Monday November 16, 2009

5:00 p.m. Welcome and Opening Remarks and Review of Evening Agenda- *Jeri Domingo-Brewer &*
Phil Huff
Roll Call; NERC Antitrust Compliance Guidelines
5:10 Overview of FERC Order on CIP Version 2 and Version 3 Procedural Steps - *Scott Mix*
5:15 Consideration of Full Group/Small Group Format for Response Document Review--*Jeri Domingo-Brewer*
5:20 Review of Strawman SDT Industry Response Document on FERC Order, CIP Version 3
7:00 Working Dinner

7:30 Continue Review of Strawman SDT Industry Response Document on FERC Order, CIP Version 3
9:00 Recess

Tuesday November 17, 2009

8:00 a.m. Welcome and Opening Remarks- *Jeri Domingo-Brewer & Phil Huff*
Roll Call; NERC Antitrust Compliance Guidelines
Facilitator review and SDT acceptance of October 20-22 Kansas City SDT meeting
summary
8:20 Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
8:25 Welcome and SDT Leadership Transition- *Jeri Domingo-Brewer & Phil Huff*
8:30 Current Membership Changes and Call for New Members - *Jeri Domingo-Brewer & Phil*
Huff
8:35 Review of SDT 706 Workplan Decisions in October, 2009 and Feedback from NERC
9:00 Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure –*Scott Mix*
9:05 Update on VSLs/VRFs- *Scott Mix*
9:10 Update on other related cyber security initiatives- *SDT Members*
9:15 Review and Refinement of CIP Version 3 Strawman Response Document
10:00 Break
10:15 Review and Refinement of CIP Version 3 Strawman Response Document
12:00 Motion to Adopt the SDT 706 CIP Version 3 Response Document *(when ready).*
12:30 Lunch
1:30 Overview of CIP 002-4 and CIP 002-009-4 Workplan - *Stu Langton*
1:40 Overview of list of CIP 002-4 Documents for posting in December.
1:45 Overview of CIP 002-4 Strawman Draft Documents, Format and Key Remaining Issues
and
Challenges- *John Lim et al. (e.g. Defining BES Subsystems; Descriptions of reliability functions; 2-3 examples of controls; and categorization of cyber systems in guidance documents).*
3:30 *Break*
3:45 Review and Refinement of CIP 002-4 Key Remaining Issues and Guidance for Drafting Groups
5:15 Organizing SDT Document Drafting Groups for Wednesday
5:30 Recess

Wednesday November 18, 2009

8:00 Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:10 Review of Key Remaining Issues and Challenges and Guidance to Drafting Groups
8:30 Convene SDT CIP 002-4 Document Drafting Groups
12:00 *Working Lunch*
12:45 CIP 002-4 Document Drafting Group Reports and Additional SDT Guidance
3:00 *Break*

3:15 Reconvene SDT CIP 002-4 Document Drafting Groups
5:30 Recess

Thursday November 19, 2009

8:00 Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15 Review and Refinement and Consensus Testing of CIP 002-4 Strawman Documents from Drafting Groups
10:00 Break
10:15 Review and Refinement and Consensus Testing of CIP 002-4 Strawman Documents from Drafting Groups
12:15 *Working Lunch*
1:00 Review and Refinement and Consensus Testing of CIP 002-4 Strawman Documents from Drafting Groups
2:45 Review and Agree on CIP 002-4 Next Steps for SDT Drafting Group(s)
Meeting Evaluation
3:00 Adjourn

Appendix # 2 Attendees List
November 16-19, 2009 Orlando, Florida

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (Friday)
2. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
3. Jackie Collett	Manitoba Hydro
4. Sharon Edwards	Duke Energy
5. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
6. Phillip Huff	Arkansas Electric Coop Corporation
7. Doug Johnson	Exelon Corporation - Commonwealth Edison
8. Frank Kim	Ontario Hydro *(Mon. & Tuesday)*
9. Rich Kinas	Orlando Utilities Commission
10.John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
11. David Norton	Entergy
12. Scott Rosenberger	Luminant Energy
13. David S. Revill	Georgia Transmission Corporation
14.Keith Stouffer	National Institute of Standards & Technology
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
16. William Winters	Arizona Public Service, Inc. (Mon., Tues, Thurs)
1. Scott Mix	*NERC*
2. Joe Bucciero	*NERC/Bucciero Assoc.*
3.Hal Beardall	*FSU/FCRC*
4. Robert Jones	*FSU/FCRC Consensus Center*
5. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

17. Jim Breton	ERCOT
18. Jonathan Stanford	Bonneville Power Administration
19. Kevin Sherlin	Sacramento Municipal Utility District (Mon., Tues, Wed)
Maureen Long,	NERC (Thurs)

SDT Members Unable to Attend

Jay S. Cribb	Information Security Analyst, Southern Company Services
Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
Christopher A. Peters	ICF International

Others Attending in Person

Bill Glynn	Westar Energy
Rick Terrell	Luminant
Chris Wright	Burns and MacDonald Engineering

Others Attending via WebEx and Phone

Rob Hardiman	Southern Company Transmission (10-20, 21, 22)
David Huff	FERC (10-20, 22)_
Justin Kelly	FERC 10-21, 22)
Hoang Neg	RRI Energy (10-20_
Jon Stitzel	Burns and MacDonald Engineering

Appendix # 3 Meeting Evaluation Summary

CYBER SECURITY ORDER 706 SDT
NOVEMBER 16-19, 2009, ORLANDO, FLORIDA
MEETING EVALUATION SUMMARY

Members used the following 0 to 10 scale in evaluating the meeting: 0= <u>totally disagree</u> and 10= <u>totally agree</u>. The results below represent the average rankings and include 12 SDT member evaluations.

1. Please assess the overall meeting.

<u>7.27</u> The agenda packet was very useful.
<u>7.75</u> The Webex document display and the audio were effective
<u>8.90</u> The quality of the meeting facility was good.
<u>7.45</u> The objectives for the meeting were stated at the outset.
<u>7.20</u> Overall, the objectives of the meeting were fully achieved.

Were each of the following meeting objectives fully achieved:
<u>9.18</u> Welcome new members and outline SDT leadership transition
<u>9.36</u> Review, Discuss and Adopt SDT Response Document to Industry Comments on CIP Version 3
<u>6.73</u> Review the CIP 002-4 and CIP 002-009-4 workplan going forward
<u>7.73</u> Receive updates on TFE, VSL/VRF and related cyber security efforts
<u>6.91</u> Review CIP 002-4 Key Issues and Provide Guidance to Documents Drafting Groups
<u>7.50</u> Convene CIP 002-4 Document Drafting Groups
<u>6.55</u> Review and refine a draft CIP 002-4 strawman and related documents
<u>7.00</u> Agree on next steps and assignments

2. Please tell us how well you believe the Team engaged in the meeting.

<u>7.09</u> The Chair and Vice Chair provided leadership and direction to Team and Facilitators
<u>8.82</u> The Facilitators made sure the concerns of all members were heard.
<u>8.82</u> The Facilitators made sure the concerns of all participants were heard.
<u>7.36</u> The Facilitators helped clarify and summarize issues.
<u>7.18</u> The Facilitators helped members build consensus.
<u>7.18</u> The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

<u>6.82</u> Overall, I am very satisfied with the results of the meeting.
<u>7.45</u> Overall, the design of the meeting agenda was effective.
<u>7.73</u> I was very satisfied with the services provided by the Facilitators.
<u>6.60</u> I am satisfied with the outcome of the meeting.
<u>6.18</u> I am satisfied with the progress we are making as a Team.
<u>7.09</u> I know what the next steps following this meeting will be.

7.18 I know who is responsible for the next steps.

4. Other comments

What did we achieve?

- Version 3 ready for posting.
- CIP002 now makes sense but more work is needed on the format.
- Comments were answered and package proposed.
- The NIST only people still don't understand about penalty's.

What are our biggest challenges going forward?

- Wasting time. The call with NERC leadership should have included the whole team. We ended up spending up extra time going over what was said and the team didn't get first hand information.
- Clean direction on CIP002.
- Format 002 so that our intent is followed.
- Develop and publish corresponding counts for high, medium and low.
- Separation of team lead and others.

What suggestions do you have for making our group more productive?

- More rigid structure. Make sure concepts are understood. Use parking lot.
- Greater use of small groups.
- The group as a whole is too large to make progress.
- Too much time is devoted in the large group to discussion and too little time to actual progress.
- Have meeting at an airport hotel only!!! That is a HUB DFW, Saint Louis, Chicago (Mid. States).

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 Subroups) 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 Subroups) 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 Subroup, 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 # 5 CSO 706 SDT Meeting Schedule

CSO 706 SDT 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 Workplan 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

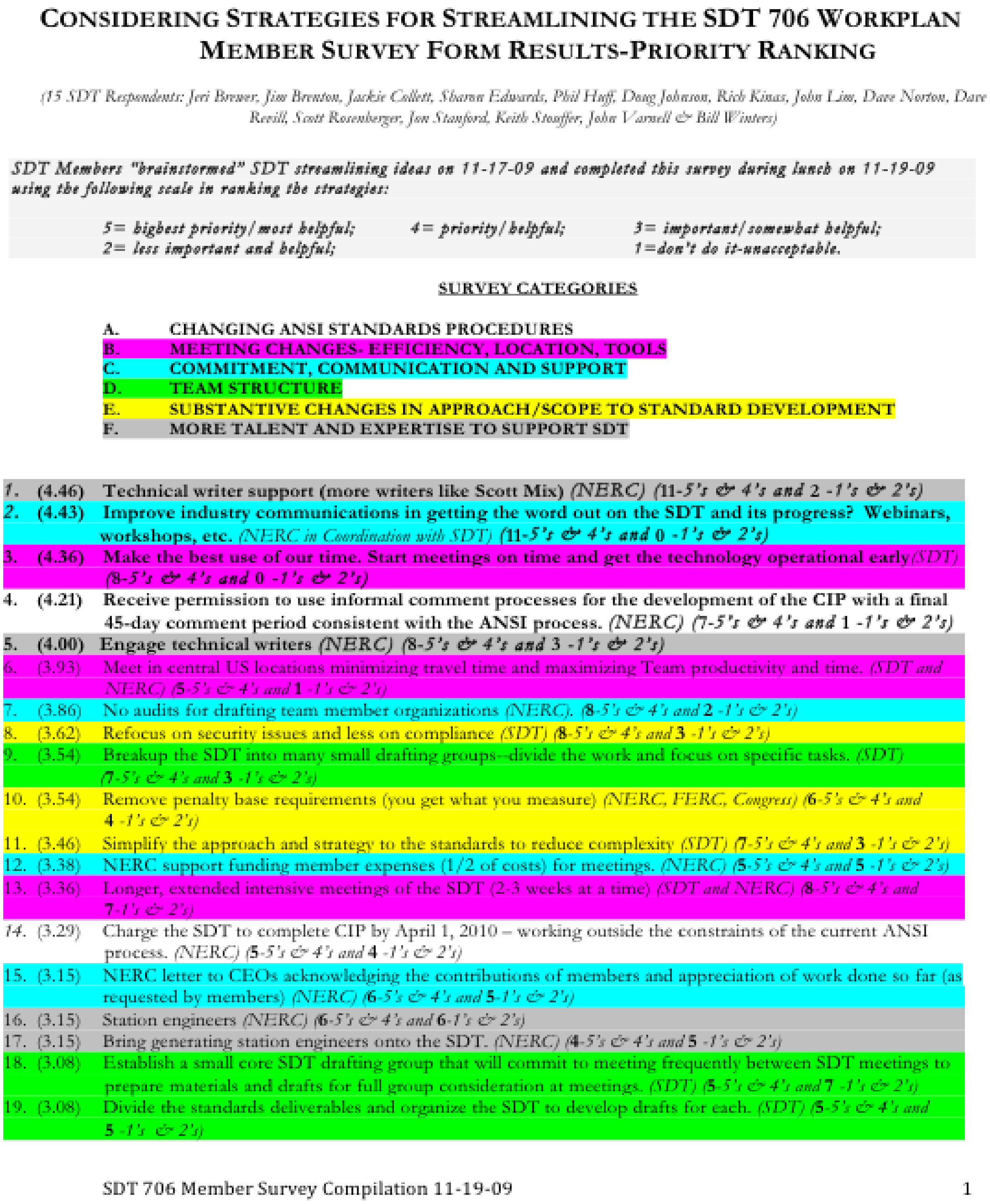
- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting

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 Prioritizing Streamlining Options



Considering Strategies for Streamlining the SDT 706 Workplan Member Survey Form Results-Priority Ranking

(15 SDT Respondents: Jeri Brewer, Jim Brenton, Jackie Collett, Sharon Edwards, Phil Huff, Doug Johnson, Rich Kinas, John Lim, Dave Norton, Dave Revill, Scott Rosenberger, Jon Stanford, Keith Stouffer, John Varnell & Bill Winters)

SDT Members "brainstormed" SDT streamlining ideas on 11-17-09 and completed this survey during lunch on 11-19-09 using the following scale in ranking the strategies:

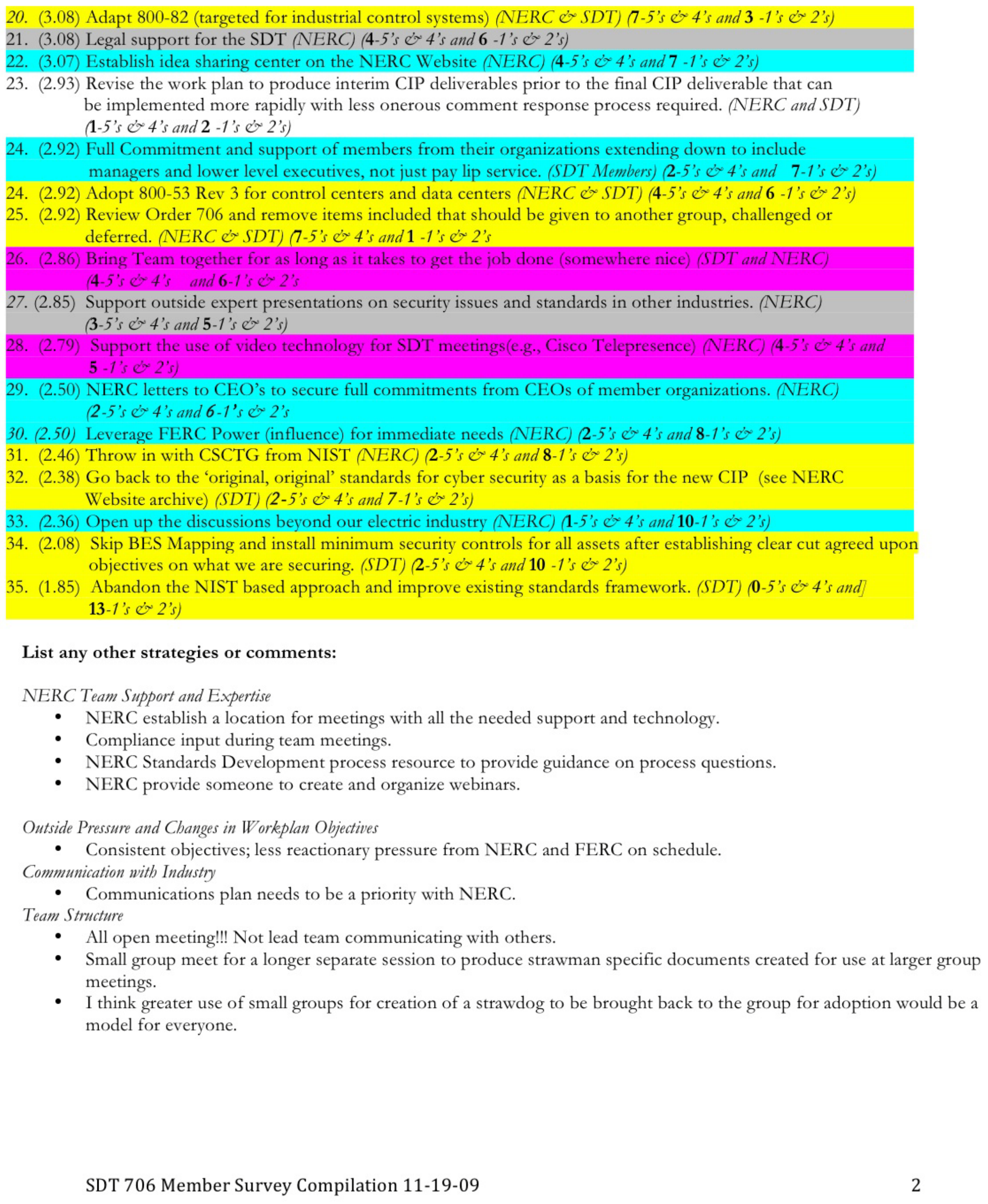
5= highest priority/most helpful; 4= priority/helpful; 3= important/somewhat helpful;
2= less important and helpful; 1=don't do it-unacceptable.

SURVEY CATEGORIES

A. CHANGING ANSI STANDARDS PROCEDURES
B. MEETING CHANGES- EFFICIENCY, LOCATION, TOOLS
C. COMMITMENT, COMMUNICATION AND SUPPORT
D. TEAM STRUCTURE
E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT
F. MORE TALENT AND EXPERTISE TO SUPPORT SDT

1. (4.46) **Technical writer support (more writers like Scott Mix)** *(NERC)* **(11-5's & 4's and 2 -1's & 2's)**
2. (4.43) **Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc.** *(NERC in Coordination with SDT)* **(11-5's & 4's and 0 -1's & 2's)**
3. (4.36) **Make the best use of our time. Start meetings on time and get the technology operational early***(SDT)* **(8-5's & 4's and 0 -1's & 2's)**
4. (4.21) **Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process.** *(NERC)* **(7-5's & 4's and 1 -1's & 2's)**
5. (4.00) **Engage technical writers** *(NERC)* **(8-5's & 4's and 3 -1's & 2's)**
6. (3.93) Meet in central US locations minimizing travel time and maximizing Team productivity and time. *(SDT and NERC) (***5***-5's & 4's and* **1** *-1's & 2's)*
7. (3.86) No audits for drafting team member organizations *(NERC). (***8***-5's & 4's and* **2** *-1's & 2's)*
8. (3.62) Refocus on security issues and less on compliance *(SDT) (***8***-5's & 4's and* **3** *-1's & 2's)*
9. (3.54) Breakup the SDT into many small drafting groups--divide the work and focus on specific tasks. *(SDT) (***7***-5's & 4's and* **3** *-1's & 2's)*
10. (3.54) Remove penalty base requirements (you get what you measure) *(NERC, FERC, Congress) (***6***-5's & 4's and* **4** *-1's & 2's)*
11. (3.46) Simplify the approach and strategy to the standards to reduce complexity *(SDT) (***7***-5's & 4's and* **3** *-1's & 2's)*
12. (3.38) NERC support funding member expenses (1/2 of costs) for meetings. *(NERC) (***5***-5's & 4's and* **5** *-1's & 2's)*
13. (3.36) Longer, extended intensive meetings of the SDT (2-3 weeks at a time) *(SDT and NERC) (***8***-5's & 4's and* **7***-1's & 2's)*
14. (3.29) Charge the SDT to complete CIP by April 1, 2010 – working outside the constraints of the current ANSI process. *(NERC) (***5***-5's & 4's and* **4** *-1's & 2's)*
15. (3.15) NERC letter to CEOs acknowledging the contributions of members and appreciation of work done so far (as requested by members) *(NERC) (***6***-5's & 4's and* **5***-1's & 2's)*
16. (3.15) Station engineers *(NERC) (***6***-5's & 4's and* **6***-1's & 2's)*
17. (3.15) Bring generating station engineers onto the SDT. *(NERC) (***4***-5's & 4's and* **5** *-1's & 2's)*
18. (3.08) Establish a small core SDT drafting group that will commit to meeting frequently between SDT meetings to prepare materials and drafts for full group consideration at meetings. *(SDT) (***5***-5's & 4's and* **7** *-1's & 2's)*
19. (3.08) Divide the standards deliverables and organize the SDT to develop drafts for each. *(SDT) (***5***-5's & 4's and* **5** *-1's & 2's)*

SDT 706 Member Survey Compilation 11-19-09 1



20. (3.08) Adapt 800-82 (targeted for industrial control systems) *(NERC & SDT) (***7***-5's & 4's and* **3** *-1's & 2's)*

21. (3.08) Legal support for the SDT *(NERC) (***4***-5's & 4's and* **6** *-1's & 2's)*

22. (3.07) Establish idea sharing center on the NERC Website *(NERC) (***4***-5's & 4's and* **7** *-1's & 2's)*

23. (2.93) Revise the work plan to produce interim CIP deliverables prior to the final CIP deliverable that can be implemented more rapidly with less onerous comment response process required. *(NERC and SDT) (***1***-5's & 4's and* **2** *-1's & 2's)*

24. (2.92) Full Commitment and support of members from their organizations extending down to include managers and lower level executives, not just pay lip service. *(SDT Members) (***2***-5's & 4's and* **7***-1's & 2's)*

24. (2.92) Adopt 800-53 Rev 3 for control centers and data centers *(NERC & SDT) (***4***-5's & 4's and* **6** *-1's & 2's)*

25. (2.92) Review Order 706 and remove items included that should be given to another group, challenged or deferred. *(NERC & SDT) (***7***-5's & 4's and* **1** *-1's & 2's*

26. (2.86) Bring Team together for as long as it takes to get the job done (somewhere nice) *(SDT and NERC) (***4***-5's & 4's and* **6***-1's & 2's*

27. (2.85) Support outside expert presentations on security issues and standards in other industries. *(NERC) (***3***-5's & 4's and* **5***-1's & 2's)*

28. (2.79) Support the use of video technology for SDT meetings(e.g., Cisco Telepresence) *(NERC) (***4***-5's & 4's and* **5** *-1's & 2's)*

29. (2.50) NERC letters to CEO's to secure full commitments from CEOs of member organizations. *(NERC) (***2***-5's & 4's and* ***6***-1's & 2's*

30. (2.50) Leverage FERC Power (influence) for immediate needs *(NERC) (***2***-5's & 4's and* **8***-1's & 2's)*

31. (2.46) Throw in with CSCTG from NIST *(NERC) (***2***-5's & 4's and* **8***-1's & 2's)*

32. (2.38) Go back to the 'original, original' standards for cyber security as a basis for the new CIP (see NERC Website archive) *(SDT) (***2***-5's & 4's and* ***7***-1's & 2's)*

33. *(*2.36) Open up the discussions beyond our electric industry *(NERC) (***1***-5's & 4's and* **10***-1's & 2's)*

34. (2.08) Skip BES Mapping and install minimum security controls for all assets after establishing clear cut agreed upon objectives on what we are securing. *(SDT) (***2***-5's & 4's and* **10** *-1's & 2's)*

35. (1.85) Abandon the NIST based approach and improve existing standards framework. *(SDT) (***0***-5's & 4's and]* **13***-1's & 2's)*

List any other strategies or comments:

NERC Team Support and Expertise

- NERC establish a location for meetings with all the needed support and technology.
- Compliance input during team meetings.
- NERC Standards Development process resource to provide guidance on process questions.
- NERC provide someone to create and organize webinars.

Outside Pressure and Changes in Workplan Objectives

- Consistent objectives; less reactionary pressure from NERC and FERC on schedule.

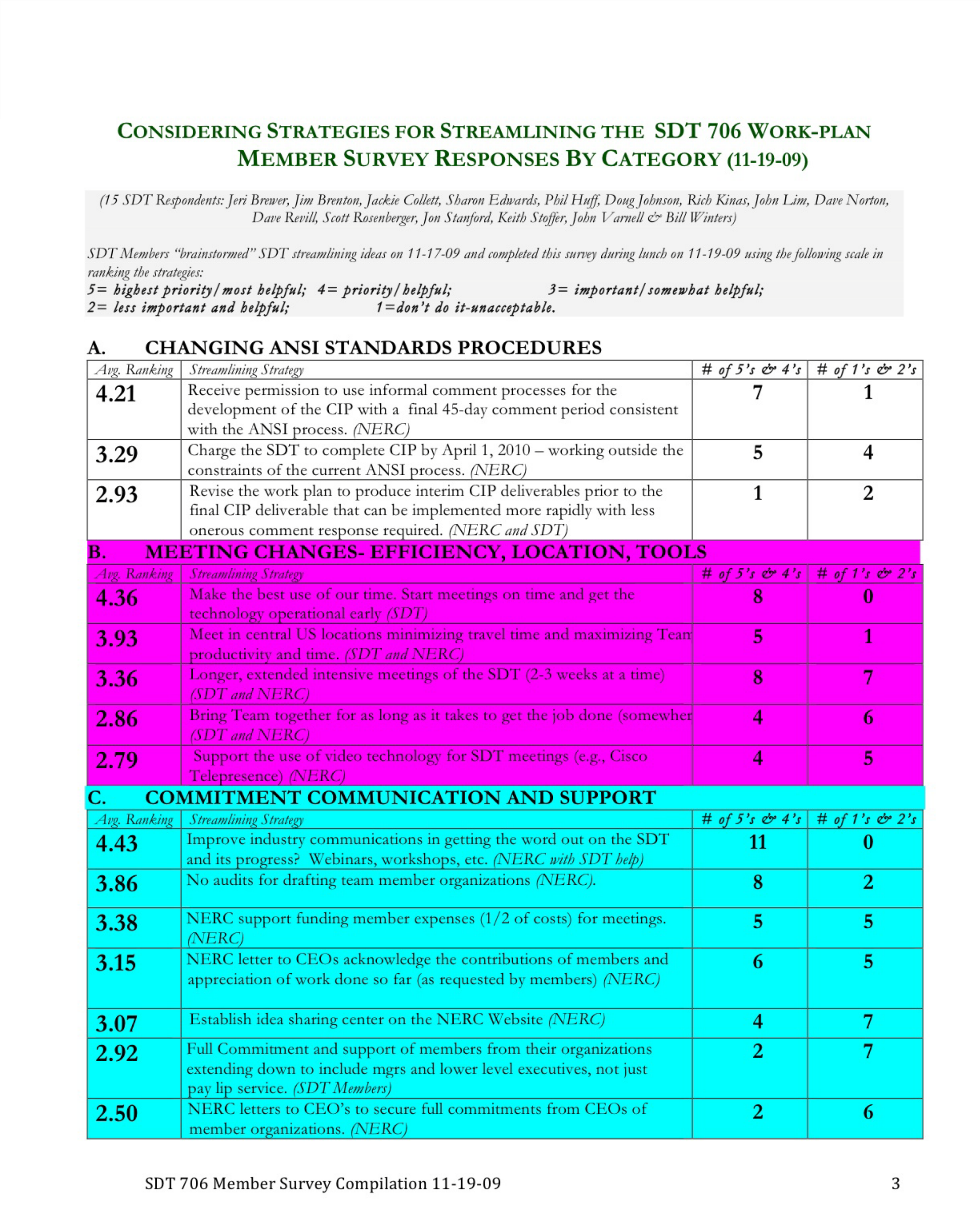
Communication with Industry

- Communications plan needs to be a priority with NERC.

Team Structure

- All open meeting!!! Not lead team communicating with others.
- Small group meet for a longer separate session to produce strawman specific documents created for use at larger group meetings.
- I think greater use of small groups for creation of a strawdog to be brought back to the group for adoption would be a model for everyone.

SDT 706 Member Survey Compilation 11-19-09 2



CONSIDERING STRATEGIES FOR STREAMLINING THE SDT 706 WORK-PLAN MEMBER SURVEY RESPONSES BY CATEGORY (11-19-09)

(15 SDT Respondents: Jeri Brewer, Jim Brenton, Jackie Collett, Sharon Edwards, Phil Huff, Doug Johnson, Rich Kinas, John Lim, Dave Norton, Dave Revill, Scott Rosenberger, Jon Stanford, Keith Stoffer, John Varnell & Bill Winters)

SDT Members "brainstormed" SDT streamlining ideas on 11-17-09 and completed this survey during lunch on 11-19-09 using the following scale in ranking the strategies:
5= highest priority/most helpful; 4= priority/helpful; 3= important/somewhat helpful;
2= less important and helpful; 1=don't do it-unacceptable.

A. CHANGING ANSI STANDARDS PROCEDURES

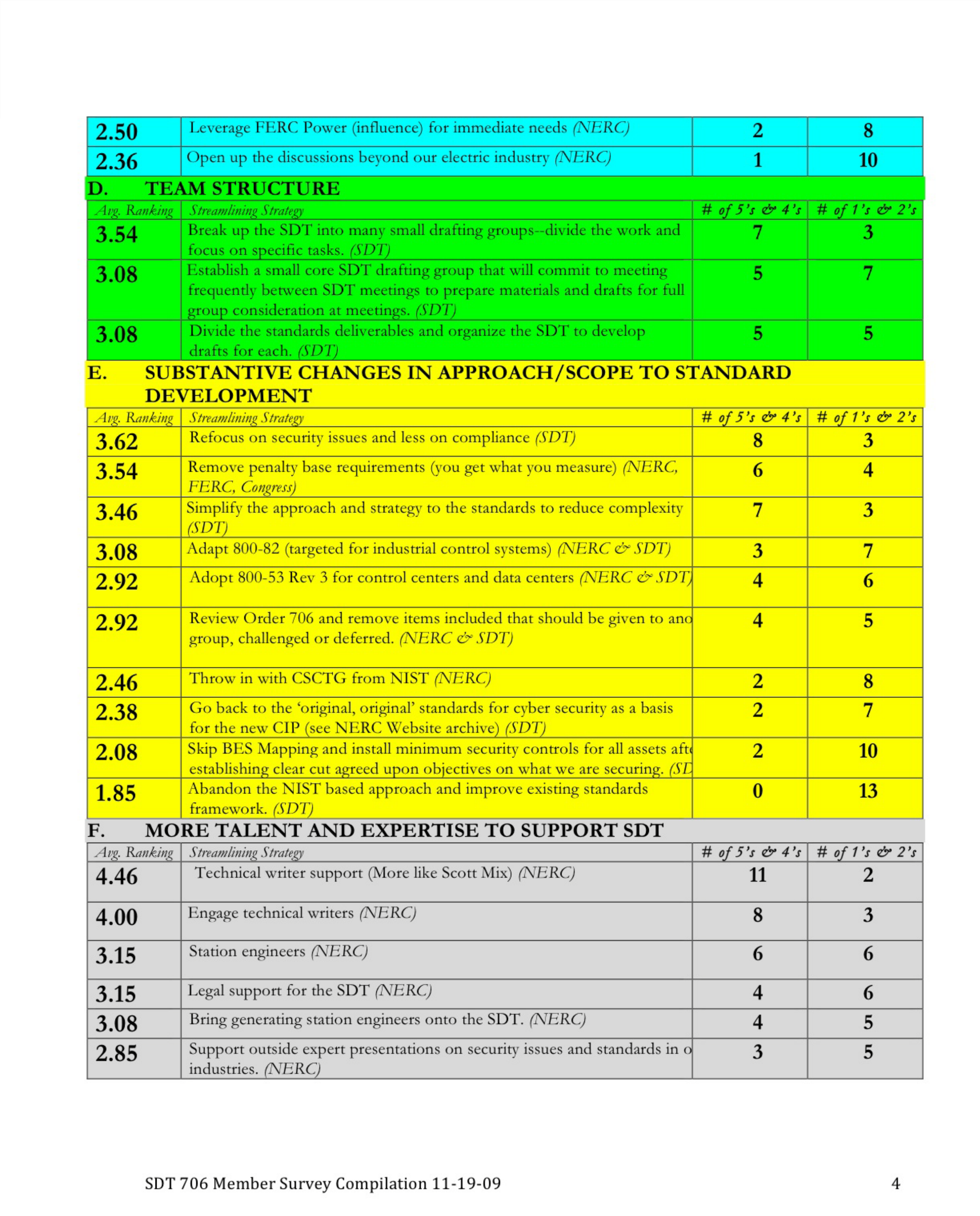
Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.21	Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process. *(NERC)*	**7**	**1**
3.29	Charge the SDT to complete CIP by April 1, 2010 – working outside the constraints of the current ANSI process. *(NERC)*	**5**	**4**
2.93	Revise the work plan to produce interim CIP deliverables prior to the final CIP deliverable that can be implemented more rapidly with less onerous comment response required. *(NERC and SDT)*	**1**	**2**

B. MEETING CHANGES- EFFICIENCY, LOCATION, TOOLS

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.36	Make the best use of our time. Start meetings on time and get the technology operational early *(SDT)*	**8**	**0**
3.93	Meet in central US locations minimizing travel time and maximizing Tean productivity and time. *(SDT and NERC)*	**5**	**1**
3.36	Longer, extended intensive meetings of the SDT (2-3 weeks at a time) *(SDT and NERC)*	**8**	**7**
2.86	Bring Team together for as long as it takes to get the job done (somewher *(SDT and NERC)*	**4**	**6**
2.79	Support the use of video technology for SDT meetings (e.g., Cisco Telepresence) *(NERC)*	**4**	**5**

C. COMMITMENT COMMUNICATION AND SUPPORT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.43	Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc. *(NERC with SDT help)*	**11**	**0**
3.86	No audits for drafting team member organizations *(NERC).*	**8**	**2**
3.38	NERC support funding member expenses (1/2 of costs) for meetings. *(NERC)*	**5**	**5**
3.15	NERC letter to CEOs acknowledge the contributions of members and appreciation of work done so far (as requested by members) *(NERC)*	**6**	**5**
3.07	Establish idea sharing center on the NERC Website *(NERC)*	**4**	**7**
2.92	Full Commitment and support of members from their organizations extending down to include mgrs and lower level executives, not just pay lip service. *(SDT Members)*	**2**	**7**
2.50	NERC letters to CEO's to secure full commitments from CEOs of member organizations. *(NERC)*	**2**	**6**



2.50	Leverage FERC Power (influence) for immediate needs *(NERC)*	**2**	**8**
2.36	Open up the discussions beyond our electric industry *(NERC)*	**1**	**10**

D. TEAM STRUCTURE

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
3.54	Break up the SDT into many small drafting groups--divide the work and focus on specific tasks. *(SDT)*	**7**	**3**
3.08	Establish a small core SDT drafting group that will commit to meeting frequently between SDT meetings to prepare materials and drafts for full group consideration at meetings. *(SDT)*	**5**	**7**
3.08	Divide the standards deliverables and organize the SDT to develop drafts for each. *(SDT)*	**5**	**5**

E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
3.62	Refocus on security issues and less on compliance *(SDT)*	**8**	**3**
3.54	Remove penalty base requirements (you get what you measure) *(NERC, FERC, Congress)*	**6**	**4**
3.46	Simplify the approach and strategy to the standards to reduce complexity *(SDT)*	**7**	**3**
3.08	Adapt 800-82 (targeted for industrial control systems) *(NERC & SDT)*	**3**	**7**
2.92	Adopt 800-53 Rev 3 for control centers and data centers *(NERC & SDT)*	**4**	**6**
2.92	Review Order 706 and remove items included that should be given to ano group, challenged or deferred. *(NERC & SDT)*	**4**	**5**
2.46	Throw in with CSCTG from NIST *(NERC)*	**2**	**8**
2.38	Go back to the 'original, original' standards for cyber security as a basis for the new CIP (see NERC Website archive) *(SDT)*	**2**	**7**
2.08	Skip BES Mapping and install minimum security controls for all assets afte establishing clear cut agreed upon objectives on what we are securing. *(SD*	**2**	**10**
1.85	Abandon the NIST based approach and improve existing standards framework. *(SDT)*	**0**	**13**

F. MORE TALENT AND EXPERTISE TO SUPPORT SDT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.46	Technical writer support (More like Scott Mix) *(NERC)*	**11**	**2**
4.00	Engage technical writers *(NERC)*	**8**	**3**
3.15	Station engineers *(NERC)*	**6**	**6**
3.15	Legal support for the SDT *(NERC)*	**4**	**6**
3.08	Bring generating station engineers onto the SDT. *(NERC)*	**4**	**5**
2.85	Support outside expert presentations on security issues and standards in o industries. *(NERC)*	**3**	**5**

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	Version 4

[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

		the NIST framework.	
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 to achieve auditable compliance.	CMEP
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 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.	TFE Filing
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	TFE Filing

		proposed.	
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	Guideline / Version 4

		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.	
31	254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-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.	Guideline / Version 4
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	Guideline / Version 4

		process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	
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 technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information	TFE Filing
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 to assure that security trainers are adequately trained themselves.	Version 4
53	443	The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide	Version 2

		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.	
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
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-	Version 4

		005-1 to require logs to be reviewed more frequently than 90 days	
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	Version 4

		constitute a modification that would require an active vulnerability assessment	
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 critical cyber assets.	Not scheduled
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	Version 2 / TFE Filing

		acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility.	
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	Version 4 / not scheduled

		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]	
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 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	Version 4 / not scheduled
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	Version 4

		data from a cyber asset prior to discarding it or redeploying it.	
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	Version 4 / Guideline

		results in a Reliability Standard that can be audited and enforced	
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 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.	Version 4 / Guideline
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	Version 4

		be in compliance with this Reliability Standard.	
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

		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)