NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

June 8, 2010, | 8 AM to 5 PM PST
June 9, 2010 | 8 AM to 5 PM PST
June 10, 2010 | 8 AM to 5:00 PM PST
June 11, 2010 | 8 AM to 12:00 PM PST

Unanimously Adopted, July 15, 2010

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

Joe Bucciero, Bucciero Consulting, LLC

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

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

CSO706 SDT June 8-11, 2010 Meeting Summary Contents

CSO706 SDT JUNE 8-11, 2010 MEETING
SACRAMENTO, CA

EXECUTIVE SUMMARY

On Tuesday morning, the Chair, John Lim welcomed the members to the SDT's 23rd meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Kevin Sherlin, a SDT member, welcomed everyone to the Sacramento, California SMUD meeting facilities and covered logistics. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3)*. The Chair reviewed the proposed meeting objectives. Bob Jones, facilitator, reviewed the proposed timed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the May 11-13, 2010 SDT session in Dallas, Texas.

Keith Stouffer, an SDT member, noted the release in the next couple of weeks of a new draft from NIST committee. Scott Rosenberger noted that Cyberstorm-3 will be taking place in the Fall of 2010 and they are looking again for volunteers.

Mr. Van Boxtel reviewed the proposed addition of an electronic voting section to the Team's Consensus Procedures with the Team. He noted it was narrowly designed to address those instances where the SDT could not secure a quorum for a face-to-face or conference call. The Team agreed to deleting the section "Posting of Industry Comment" as it would only apply to informal industry comment postings and agreed to extend the time for decision in the email vote procedure from 4 to 12 hours. The motion passed with 17 yeas and 1 nay. Dave Revill noted his concern was that the procedure was too narrow in that it did not allow electronic vote for posting documents for comments or ballot.

The SDT reviewed and discussed the schedule and work plan at several points during the Sacramento meeting. On Tuesday there was a discussion generally on the current plan that the Team adopted in May, 2010 to complete work and post for formal comment CIP 010 and 011 at the conclusion of the Pittsburgh meeting in July, 2010.

Phil Huff presented a draft schedule for the next four weeks to complete its work in Pittsburgh and file the CIP 010 and CIP 011 for formal comment and balloting. He noted the necessary deliverables including: CIP 010 and 011 standards/requirements; VSL's, measures, guidance document; FERC directives summary; CIP version 3 mapping; informal comment summary; and comment form for the formal comment posting.

Bob Jones summarized the context for the schedule which the Team had discussed noting the possibility of two rounds instead of three and using the additional time to improve product. Stu Langton reviewed the dynamic current political context and the need felt to demonstrate that the industry can produce a good product in a reasonable amount of time. However, as the Team has discussed, once it sends the standard out for the first ballot they will lose flexibility in making changes.

It was noted that the Standards Committee was meeting concurrent with the SDT's Tuesday morning discussion. Following lunch on Tuesday, Howard Gugel reported to the Team on the Standards Committee call. He noted that NERC President Gerry Cauley and Standards Committee Chair Alan Mosher felt strongly a need to present some cyber security standards changes to FERC and Congress by the end of the year. CEOs in the industry have expressed concern that CIP 010 and 011 may not pass by end of the year and that there may be a need for a "Plan B" which might take CIP-010 with high and medium bright lines and then add CIP-003-009 as is. Jason Marshall noted that President Cauley is focused on responding to Congress.

Phil Huff reported on the Sub-team leads lunch discussion regarding schedule adjustments – think complete revisions based on comments by July, push formal posting until after August – it is not feasible to post prior to August 20th – also assumes support from NERC staff for drafting and adjusting the membership on some sub teams. The SDT Leadership will talk to standards committee and NERC management to seek pushing the initial posting back 31 days from the current plan which would mean the Chicago meeting in August. The end of year deadline depends on the level of industry acceptance in formal posting and ballots.

After discussion about the time frame and content the facilitators suggested a straw poll on different extensions of time assuming the same SDT monthly meeting schedule and interim conference calls and assuming that all FERC directives will be addressed including the "Post Version 4" directives. Members expressed their preferences among one of three options. Each option included the 38 days to the Pittsburgh meeting plus:

- **Option A.:** adding 30 more days, that is to the SDT Chicago meeting-August 10-13, (Sub-team leads proposal) and then to initial ballot – **2 members**.
- **Option B:** adding 60 more days, that is to the SDT Winnipeg, September 7-10 meeting, and then to initial ballot – **8 members.**
- **Option C**- adding 90 more days, that is to the SDT Toronto October 12-15 meeting, and then to initial ballot – **12 members.**

Following this, John Van Boxtel proposed a motion that was discussed and revised as follows:

> Based on the results of industry feedback from the informal comment period, and the need to send a quality product out to the industry to gain acceptance of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff identifying these issues and ask for an extension for the posting of the CIP draft standards in October 2010 to be added to the schedule to develop the CIP-010 and CIP-011

The Vote on the motion to adopt was: **11 yea – 5 nay (69%).**

Bob Jones suggested that the SDT is unanimous that it needs more time to do a quality job based on the industry comments, Order 706 directives and FERC comments. The Chair thanked the Team and suggested the Chair and Vice Chair would take this as guidance in their discussion on Friday morning with the Chair of the Standards Committee.

On early Friday morning, John Lim and Phil Huff reported to the SDT on a conference with the chair of the Standards Committee, Allen Mosher. They discussed with him the time and schedule for the CSO706 Project, and the Standards Committee was agreeable to a 90 day extension to complete the CIP-011 work if there could be a CIP-010 product going out to industry in July. Mr. Mosher requested the SDT to create a schedule for moving forward with both CIP-010 and CIP-011, and he suggested that in the interim until implementation of CIP-010 and CIP-011 that the SDT use an amended CIP-002 to address the issue of critical assets. Phil noted that he and John raised the remaining Order 706 directives issue, and Mr. Mosher understood the difficulty of getting both out by end of year but expressed the need for something by end of year if not the full package.

Phil Huff reviewed with each of the Sub-teams where each team was in summarizing the comments. Three teams are still working on summaries while others have identified key issues. None have moved on to consider how to address the comments and changes to the requirements. He noted that there was a possibility, if needed, to split up Jay Cribb's team into two sub-teams (005 and 007) and he would consult with Jay and other team members before a decision was made.

Following the morning call with the Standards Committee leadership, the SDT Chair and Vice Chair decided to schedule a SDT conference call meeting to discuss a proposed new schedule.

Bob Jones reviewed the documents compiled for the SDT's review of industry comments. He summarized an overall set of results showing the percentage of support or opposition for key components and questions. Scott Mix had sent out over the weekend a "consideration of comments" document that included over 900 pages.

The Chair noted that the Team received a significant amount of input from the industry and FERC since the posting, and the SDT will need to review and consider what kinds of revisions may be needed for the CIP-010 and CIP-011 requirements based on these comments and the SDT's continuing development of these requirements. He noted that the next phase will include a pre-ballot review followed by formal ballot, and underscored the point that there is a lot of work ahead of the SDT. The comment period closed on June 3, which did not give the SDT much time to review the comments prior to the Sacramento meeting. The SDT will need to rely on and trust that Sub-Teams will work to address the comments and share with the full SDT their summary of those comments.

The Team has maintained an ongoing "parking lot", a table list of issues raised in the course of the development and discussion of CIP-010 and CIP-011, and as part of the SDT's review of the industry comments. These were presented and discussed by the Team and a table that defines these issues and identifies how they were or will be resolved or handled going forward is included as an appendix to this summary.

Joe Bucciero provided the SDT with a meeting summary that offered an overview of the FERC/SDT meeting held on May 27th at FERC's offices in Washington, DC (*See Appendix #X)*. John Lim noted that the atmosphere for the meeting was cordial and professional, and the meeting brought forth constructive input and ideas. In general, FERC staff agreed with the approach taken in the draft CIP-010 and CIP-011 standards, but acknowledged that a lot of work is still needed in clearly defining the requirements. Joe noted that FERC staff expressed the following issues and concerns:

- The Low impact level requirements are insufficient and need to be bolstered, i.e. the Low baseline is too low.
- The proposed 36-month review cycle for the impact categorization needs to be shortened, at least for the first review cycle (possibly to 12 months).
- Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.
- The bright line thresholds stated in Attachment II need to be justified or at least explained.
- The SDT must ensure that all of the requirements are auditable.
- Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the significant effort being performed by the SDT in creating these standards. Jan Bargen, FERC, noted that they recognize the considerable amount of work of the SDT so far, but believes there is still more to be done including both the justification and baseline issues – e.g., how do you address the minimum requirements, are we moving forward if more of the electric system is not covered, need to explain why this is better. There are too many items not currently included. What else is being brought in to the new standards? Is the baseline for protection of BES equipment set at the right level. The SDT also discussed the issue of "immediate revocation", the baseline for Low Impacts, Physical Security, bright lines, and avoiding the prescriptive (how) in drafting standards.

The SDT also held an industry technical workshop in Dallas, TX on May 19-20, 2010 as a form of outreach to the industry concerning the new cyber security requirements. The Chair noted that this was the first time NERC has used such a workshop in the context of a standards development process and any lessons learned would be helpful for NERC to consider.
He suggested that there was excellent industry turnout for the workshop, and some excellent questions were raised and suggestions offered that the SDT should consider going forward. The Team discussed ways to make future workshops more interactive.

The Chair proposed that the Sub-teams meet to review and summarize industry comments and report back to the full SDT.

Bob Jones presented an overview of Industry responses for Question 9 regarding the format for CIP 011.

CIP 011 COMBINED REQUIREMENTS FORMAT

	Totals	*%*
Keep CIP 011-1 as one document-	(48)	40.3 %
Break CIP 011-1 into multiple standards	(38)	31.9 %
No preference-	(23)	19.3 %
Not checked -	(10)	8.4 %
Total:	(119)	100

Keep CIP 011-1 as one Document- Comment Topics

1. Better Organization and Organizational Review *(8 comments)*
2. Auditing and Multiple Violations of Single Standard *(6 comments)*
3. Format *(2 comments)*
4. Table Format *(1 comment)*
5. Revisions *(1comment)*
6. Alignment with Other Standards *(1comment)*

Break up CIP 011-1 into Multiple Standards- Comment Topics

1. Retain CIP-003-009 Format *(10 comments)*
2. Audit/Enforcement/Compliance and Negative Perceptions *(9 comments)*
3. Suggested Standard Format Combinations *(8 comments)*
4. Level of Effort and Cost of Changing Format *(6 comments)*
5. Use Functional Areas *(3 comments)*
6. Consistency with Other Industry Cyber Protection Standards *(2 comments)*
7. Makes Easier Ownership Assignment and Referencing *(1 comment)*
8. Monitoring Changes *(1 comment)*
9. Aids the Revision Process *(1 comment)*
10. Focus on Security *(1 comment)*
11. Approve as a Complete Set *(1 comment)*
12. CIP Standards Should Stand Alone *(1 comment)*

No Preference or Not Checked- Comment Topics

1. Implementation, Updates and Revisions *(4 comments)*
2. Focus on Defining Auditable Requirements *(3 comments)*
3. Reporting at a Requirement Level *(2comments)*
4. Simpler Management *(2 comments)*
5. Table Format *(1comment)*

Stu Langton reviewed with the SDT four key comments *(see below)* noting EEI and APPA represent approximately 60% of the industry. What are their arguments? Ameren suggests it will be easier to find requirements in one standard and use. EEI argued for the legacy of CIP-003-009 or at least a way similar to it as being easier for the industry to recognize and preserve sunk costs. APPA suggested sub-headings in CIP-011 are illustrative of the need to separate into multiple standards and that multiple standards would be simpler to work with and revise in the future. IRC suggested functional areas with each standard being a stand-alone. The discussion of these comments covered issues related to Compliance Enforcement and Reporting.

The facilitators initially suggested first taking a straw poll on which of the two formats members favored then ask members for propose a motion on the format. The straw poll resulted in 10 members favoring multiple standards (CIP-011 to CIP-021) based on the eleven sections of the CIP-011 standard, and 9 members favoring the one standard format of CIP-011. Following this there was a motion (Doug Johnson, second by John Lim) to adopt multiple standards (CIP-011 to CIP-021) resulting in 11 yeas (61%) and 7 nays (39%). The facilitators suggested revisiting this question at a later point noting the sentiment on the Team has appeared to shift in favor of multiple standards for CIP-011, but it fell short of the 75% needed to make a SDT decision on this question.

John Van Boxtel provided an initial presentation on a possible improvement in the format utilized for definition of the CIP-011 standard. He provided an overview of the standard format used by PCI (DSS standard format).

The facilitators reviewed the process for reviewing the group reports which presented summaries of the industry comments for each of the 54 questions in the Comment Form. He noted that he wants each sub-team to help ensure that we have identified the right issues and determine who needs to address them.

Phil Huff reviewed with the Team the responses to Question #54. There included comments on clarity or wording; on definitions especially hourly: moving definitions to NERC glossary, appreciate local definitions, separate attachment for all local definitions; timing issues; implementation plan –about “gap” in compliance programs, sufficient time for categorization, CIP-010 may require more time; categorization issues; consistency issues.

Phil Huff provided the overview for Question #53 including 66 comments, with 57 specific comments addressing: TFEs (passwords, malicious code, appropriate use, system hardening, security event monitoring, wireless and remote address, communication and date integrity) device characteristics, write clear requirements, and TFE process improvements.

John Lim provided the overview of industry comments for CIP-010 focusing on three questions: #1 – definitions, #6 – the Attachment 1 functions, and #7 – Attachment 2 categorization of BES cyber assets. Jim Fletcher presented a summary of the industry responses for question #6 with 58% of industry agreeing but suggesting the attachments need more definition, examples, and guidance especially in Attachment 1.

Rod Hardiman presented a summary of the industry responses to Question #7 including that 75% of the respondents disagree.

Dave Revill introduced his Sub-team's work noting it covered Questions 11 on Security Governance and Policy, and Questions #40-48. Question #47 on BES Cyber System maintenance included concerns about the interaction between the list of personnel in Table 26.1 and the lists granting authorized electronic and physical access; about the interaction with other user/account management requirements; regarding the allowance for emergency maintenance situations; requirements on maintenance devices should include system hardening; all maintenance devices should be documented in a list; and Ensure that systems used for maintenance do not act as an unauthorized access point. He noted they also received comments on the definition of "maintenance" – some said to consider that any temporary connection also have appropriate controls.

Sharon Edwards presented the following summary of industry comments on Question 17, Electronic Access control which included: Need a strategy for designing baselines by impact levels – we missed the mark; revocation of access – do not like the time parameters for revocation, transferred personnel should not be treated as risk, and clarify when the clock starts for no longer needing the access plus a distinction should be made in the standard between "primary" access and "secondary" access; clarity and definitions on acceptable use, account types, system access, remote access, external connectivity, wireless, etc.; separate remote and wireless access; consistency; and quarterly review is excessive.

Scott Rosenberg presented the overview of industry comments on response and recovery including: Guidance on cyber security incident classification highlighted; Definitions; Incident response for low impact or non routable connections should be removed; Consistency between requirements related to impact level; Single versus multiple incident response plans and testing issues; Combine incident response testing and review/update; Review results of incident response tests in other than 60 days; Recovery testing; Data retention identification requirements of personnel responsible; Coordination of physical aspects of cyber security incidents; Incident response and recovery plan reviews and question around changes required; Suggestions for re-wording; and Coordination of backup plans.

Jay Cribb noted and summarized the industry responses to System Security Questions #35-39 which covered more than 100 pages and addressed: malware prevention; patch management; system hardening; data and communications integrity; boundary protection and system boundary; and protective systems.

Doug Johnson presented the summary of industry comments on personnel and physical security including Question #12, R2, R3 R4, R5 and R6.

On Thursday the Team took up how to address FERC Order 706 issues that have been termed "post Version 4 issues" that include:

- Access Control Redundancy/~~Defense in Depth~~ (two or more diverse security measures in constructing electronic and physical security perimeter)
- Active vulnerability assessments every three years
- Forensic data collection

The Team agreed that it will take time to address these issues, but they should be included in the provisions of CIP-010 and CIP-011 if the SDT has some more time to complete the task. The SDT agreed they need to reach out to experts for assistance (e.g., Carnegie Mellon on Forensics) and increase the two-way communication concerning what FERC is asking for, i.e., the intent of the request. Jan Bargen, FERC, noted her understanding is that you do not have cyber security if you do not have security in-depth – too severe an interpretation that it has to be all or nothing and cannot been done in pieces – you can explain progress and point to it in the requirements and note what else needs to be worked on – recognize you are working on a new paradigm and have a window of opportunity.

Scott Mix presented the implementation plan concepts and approach. The Team asked him to develop and present options for proceeding.

On Thursday, Scott Mix offered the following Implementation Plan options for the SDT's consideration and consensus testing was performed on the options by the SDT:

1. Multiple fixed dates (based on connectivity and dependent on impact level)
   4 -6; 3 -8; 2 -5; 1-0 = **58 (3.2 of 4)**

2. Entity-specific implementation plan
   a. need to develop boundaries and approval guidance
   b. resource issues at regions for approving plans
   c. multiple versions in play at the same time for audits
   d. will require "true-up" of CIP 011 requirements for connectivity, etc.
   e. consistent with current NGP plans
   4 -3; 3 -11; 2 -4; 1 -1 = **54 (2.8 of 4)**

3. Single fixed date (independent of impact level)
   4 -4; 3 -9; 2 -3; 1 -2 = **51 (2.8 of 4)**

4. Fixed date for each requirement, for each impact level
   a. some requirements would be the same for all levels
   b. may have issues with "early compliance"
   c. will require a separate plan for NGP
   4 -0; 3 -1; 2 -14; 1 -4 = **35 (1.8 of 4)**

The Team discussed the low impact baseline and how to provide more detail in the standard including featuring the baseline in each table for each requirement.

Following the Sacramento meeting it was agreed there would be a need for weekly sub-team meetings and possible sub-team leads meetings. Later in June the schedule would be adjusted to reflect this and include some SDT meetings to develop drafts for NERC staff to review in advance of the July meeting in Pittsburgh. The Chair suggested convening the SDT to review a new draft schedule the following week once more information was available from NERC and the Standards Committee.

The Chair thanked SMUD and especially Kevin Sherlin for his excellent support for the SDT in hosting this meeting.

The meeting adjourned at 11:00 p.m. on Friday, June 11, 2010

23RD MEETING SUMMARY

Cyber Security Order 706 SDT — Project 2008-06
June 8-11, 2010
Sacramento, CA

I. AGENDA REVIEW, SDT WORKPLAN AND CONSENSUS PROCEDURES

A. Meeting Objectives and Agenda Review

On Tuesday morning, the Chair, John Lim welcomed the members to the SDT's 23rd meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Kevin Sherlin, a SDT member, welcomed everyone to the Sacramento, California SMUD meeting facilities and covered logistics.

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.

The Chair reviewed the following proposed meeting objectives:

- To review the CSO 706 SDT 2010 Work plan and Schedule;
- To review and adopt CSO 706 SDT 2010 Consensus Procedures draft;
- To receive updates on other related cyber security initiatives;
- To review the results of the FERC/NERC May 27 Meeting;
- To review the results of the May 19-20 Dallas Technical Workshop;
- To review the documents to be produced for the July, 2010 CIP posting;
- To receive an overview of the industry informal comments on CIP 010 and 011;
- To review industry input on the CIP format and to test SDT consensus on CIP format going forward;
- Sub-teams review industry input from the Technical Workshop and informal comments and propose any potential changes in the draft standards;
- SDT reviews Sub-Team reports on industry input from workshop and informal comments and any proposed changes in the draft standards;
- To review progress on the Implementation Plan Drafting Group and the Guidance Document Drafting Group; and
- To agree on next steps and assignments

Bob Jones, facilitator, reviewed the proposed timed meeting agenda *(See appendix #1*).
On Thursday morning the SDT approved without objection the meeting summary for the May 11-13, 2010 SDT session in Dallas, Texas.

B. Related Cyber Initiatives

Keith Stouffer, an SDT member, noted the release in the next couple of weeks of a new draft from NIST committee. Scott Rosenberger noted that Cyberstorm-3 will be taking place in the Fall of 2010 and they are looking again for volunteers. John Van Boxtel noted that there is a concern that the result is already pre-determined. Gerry Freese suggested that even if it is pre-determined it is a good experience for people to better understand circumstances.

C. Review and Adoption of Revised SDT Consensus Procedures

At the Dallas SDT meeting, the Team reviewed some proposals for updating the consensus procedures originally adopted by the Team in November, 2008. At the conclusion of the discussion, the Chair asked John Van Boxtel and Bill Winters to serve as a drafting team and address the email voting procedure.

Mr. Van Boxtel reviewed the proposed addition of an electronic voting section with the Team *(See Appendix #5)*. He noted it was narrowly designed to address those instances where the SDT could not secure a quorum for a face-to-face or conference call and "will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote."

The Team agreed to deleting the section "Posting of Industry Comment" as it would only apply to informal industry comment postings and agreed to extend the time for decision in the email vote procedure from 4 to 12 hours.

Jon Van Boxtel made a motion which Dave Norton seconded to adopt the proposed revisions. The motion passed with 17 yeas and 1 nay. Dave Revill noted his concern was that the procedure was too narrow in that it did not allow electronic vote for posting documents for comments or ballot.

II. REVIEWING THE CSO 706 SDT PROCESS AND SCHEDULE

A. Initial SDT Workplan Review

The SDT reviewed and discussed the schedule and work plan at several points during the Sacramento meeting. On Tuesday there was a discussion generally on the current plan that the Team adopted in May, 2010 to complete work and post for formal comment CIP 010 and 011 at the conclusion of the Pittsburgh meeting in July, 2010 (*See Appendix #4)*.

Members and Participants Discussion Comments

- Are we talking about from now until early July to have weekly meetings? FERC recognized our schedule is ambitious. Before the SDT last posting in April the time crunch pushed members to vote yes even thought they still had questions and concerns to address and resolve.
- Jan Bargen, FERC, noted that the work plan schedule is aggressive and that FERC staff is interested in a quality product that represents the next cyber security paradigm for the industry and addresses the directives. Perhaps at the end of this meeting, the SDT needs to assess if they can get there or not – assess what it can do in the time – or express what could be done by when. Between now and the formal posting is the best time to improve the product.
- Mike Keene, FERC, noted that FERC staff would prefer a better product later than meeting a self imposed deadline – they would rather wait six months if necessary to get a quality result to review.
- NERC staff noted that NERC President Gerry Cauley has "put a stake in the ground" that the SDT, NERC and the industry will have a cyber security product approved by industry to present to FERC by the end of 2010 that would indicate the progress the industry is making in this area.
- NERC put in that schedule – if we could change President Cauley's mind, how could we get an extension of time without a new order?
- In the Short term between now and Pittsburgh there are 38 business days.

B. Proposed Revised Schedule

Phil Huff presented a draft schedule for the next four weeks to complete its work in Pittsburgh and file the CIP 010 and CIP 011 for formal comment and balloting. He noted the necessary deliverables including: CIP 010 and 011 standards/requirements; VSL's, measures, guidance document; FERC directives summary; CIP version 3 mapping; informal comment summary; and comment form for the formal comment posting.

Member Comments

- This is unrealistic – initial revisions of the requirements by the Sub-teams to NERC staff by end of next Tuesday? Then one week to compete?
- We haven't fully documented the industry informal comments to be addressed and only two days for meeting and finish, two days not already on our calendars – this is not ambitious, it is impossible.
- If Tuesday is unrealistic can the Sub-teams target of COB on Friday of the following week for revisions to requirements but send as they become available to Howard with June 18th deadline to complete all revisions?

Difficult to get this done if different sub teams are on different pages – how do we get the whole SDT onto the same page. We can get material out but are we trying to get this right?

- In addition, there are several cross and coordinating issues that have not been addressed and these may not possible to work out by next Friday.

Bob Jones summarized the context for the schedule which the Team had discussed noting the possibility of two rounds instead of three and using the additional time to improve product. Stu Langton reviewed the dynamic current political context and the felt need to demonstrate that the industry can produce a good product in a reasonable amount of time. However, as the Team has discussed, once it sends the standard out for the first ballot they will lose flexibility in making changes.

Member and Participant Discussion Comments

- If the SDT turns out a product industry cannot live with they will vote it down – the Team needs time to get it right than get it out sooner but wrong – lot of frustration that process will result in a changes that will not bring security and increase compliance problems.
- This has to be right. We can't allow ourselves to be beat into submission by politicos who do not understand the cyber security system – we are industry volunteers with real jobs.
- In light of the substantial level of informal comments, we can imagine the time needed in the formal comment phase and we have to respond to each comment.
- Can the July posting be another informal so we can address without responding to every single one?
- Want to propose the Team changes the deadline – sub-team leads can meet over lunch to determine how much additional time is needed?
- In the industry, if we know we cannot hit deadline with a good product, we change the deadline and add resources. Can the SDT get others (NERC staff) to review and compile the comments?
- Not sure clerks could have done the job – we have a window to get it right – the proposed schedule is too brittle and short and will not allow us to create a quality product. We should not live with a schedule dictated to us or have others determine what is the time needed. NERC executives do not fully understand the situation.
- Jan Bargen, FERC staff, noted that at the May 27th FERC meeting, FERC staff expressed concern that we need a quality product. The deadline at the end of the year is not being imposed by FERC.
- There is consensus in the room for a new deadline that provides for more time to get it right.
- We need to be careful and keep our focus is on reliability of the BES – not serving the industry with a less than quality product. It is not serving industry to remove an opportunity for comments – only two balloting periods is not realistic given the substantive change reflected in CIP 010 and 011.

- We need a motion to request a new deadline from NERC.

C. Standards Committee Input

It was noted that the Standards Committee was meeting concurrent with the SDT's Tuesday morning discussion. Howard Gugel was on that call and will bring back information. Might be wise to give him a chance to fill in context before moving forward. The Chair noted that if the SDT requests an extension, we will need to give an alternative schedule saying what we think it will take to get it done and by when. Phil Huff proposed meeting with the Sub-Team leads over lunch to discuss possible ideas for alternative schedule.

Following lunch, Howard Gugel reported to the Team on the Standards Committee call.
He noted that NERC President Gerry Cauley and Standards Committee Chair Alan Mosher felt strongly a need to present some cyber security standards changes to for FERC and for Congress by the end of the year. CEOs in the industry have expressed concern that CIP 010 and 011 may not pass by end of the year and that there may be a need for a "Plan B" which might take 010 with high and medium bright lines and then add CIP 003-009 as is. Jason Marshall noted the President Cauley focused on responding to Congress.

Member Discussion Points

- This idea is to present "something" by end of year? Posted and balloted or just making progress?
- This is "something approved by industry to show Congress and FERC of progress being made.
- Does NERC have a plan B to finish this work or this team being asked to prepare a plan B? It is not clear.
- "Something" that meets deadline that also meets industry and Congressional concerns?
- Plan B may refer to perception on the Hill that industry has not responded to their concerns – such a plan may kick in after first ballot if the first ballot indicates an unreasonably low level of acceptance and low expectation of passage.
- There has not been much discussion of how 706 directives will be addressed by this "Plan B"-- 010 with CIP 003-009 package.
- The "Plan B" approach may be doable and can address 706 which points out what to address in the existing structure.
- We should consider a motion to draft a letter to NERC requesting an extension.

D. Sub-Team Leads Review of Schedule Needs and Review of Options

Phil Huff reported on the Sub-team leads lunch discussion re schedule adjustments – think complete revisions based on comments by July, push formal posting until after August – it is not feasible to post prior to August 20th – also assumes support from NERC staff for drafting and adjust membership on some sub teams – leadership talk to standards committee and NERC management to seek pushing posting back 31 days from the current plan which would mean in Chicago in August. The end of year deadline depends on the level of industry acceptance in formal posting and ballots.

After discussion about the time frame and content the facilitators suggested a straw poll on different extensions of time assuming the same SDT monthly meeting schedule and interim conference calls and assuming addressing all FERC directives including the "Post Version 4" directives. Members expressed their preferences among one of three options. Each option included the 38 days to the Pittsburgh meeting plus:

- **Option A.:** adding 30 more days to the SDT Chicago meeting-August 10-13 (Sub-team leads proposal) then to initial ballot – **2 members**.
- **Option B:** adding 60 more days to Winnepeg, September 7-10 SDT meeting, September and then to initial ballot – **8 members.**
- **Option C**- adding 90 more days to the SDT Toronto October 12-15 meeting- October and then to initial ballot – **12 members.**

SDT Discussion of Straw Poll

- Jay Cribb's issues may have an underlying problem of agreement that time alone may not address. May need to consider a change the members in the group to facilitate development of the requirements.
- Need a clearer rationale. E.g. discovery that industry is concerned abuot the post v4 issues discussed earlier which FERC has directed NERC to address.
- This is a request to extend time when the first formal posting takes place. We need time and full meeting to address comments and refine draft requirements.
- Also discussed shuffling to share the work load among the teams
- Feel 31 days is too short – need time to discuss and then develop guidance too – I can give another week in this month but not more – I think we need at least two more face to face meetings.
- June 2011 for end (a six month extension). If you go to the well, better be sure we get enough water.
- Assume that all of these options include a request for additional help from NERC. We can request it, but we may not get it

Following this, John Van Boxtel proposed the following motion, with Doug Johnson as a second.

> **1st Motion:** "Due to the amount of work remaining, and the need to send a quality product out to the industry to gain acceptance of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff asking for additional time to be added to the schedule to develop the CIP 010 and CIP 011 standards."

SDT Discussion Motion #1

- We need to state exactly what we are asking for – need team agreement on the time we are requesting and then add to the motion Concerned about only 31 days – not sure what we need but the schedule is tight and brittle – need to ask for more time, how much is still open but needs to be answered before sending the letter – industry comments suggest a lot of work.

- John noted he was amenable to a specific time frame being added to the motion.

Revised Motion #1: Based on the results of industry feedback from the informal comment period, the desire to address the FERC 706 directives (including the former post Version 4 issues), and the need to send a quality product out to the industry to gain acceptance of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff identifying these issues and ask for an extension for the posting of the CIP draft standards in October 2010 to be added to the schedule to develop the 010 and 011

Discussion of 1st Revised Motion #1

- Concerned about putting in "706" reference without saying "fully address" – okay with post v4 issues.
- Suggest putting such details in the letter to be drafted if motion passes.
- Not comfortable with the parenthetical related to post version 4 issues –this was covered by "fully address all"
- Question is the end date – asking for an end date to deliver to FERC?
- However, the end date is not in your control – discussion is how much time will it take the SDT to get to first formal posting.
- Asking Standards Commission for permission will get a "no". We should advise them we need more time and move forward with that schedule unless we hear otherwise from the Committee.
- Writing a letter starts a conversation – need communication between our leaders and NERC management – also need more resources to support volunteer effort – just agree to ask our leaders to seek extension from management to assure quality product.
- The Chair and Vice Chair have a conference call Friday morning with Standards Committee Chair. They need guidance on how much time we need – 90 days to complete the work in front of them based on comments and input from FERC – more staff is not the issue.
- Possible scenario – ask for more time for 010 and 011 and they go with plan B of 010 and CIP 003-009 for balloting process.
- Plan B would be voted down
- The scenario doesn't make sense – if we are struggling, the industry will not understand that plan B proposal.
- How much time will it take us to responsibly post for formal comment?
- Plan B will take it out of the hands of the drafting team/
- The more time we ask for, the more likely it is to be denied and taken away to assign plan B to be developed elsewhere.

John Van Boxtel (and Doug Johnson as a second) agreed to the following in light of the discussion as friendly amendments:

> 2nd **Revised Motion #1:** Based on the results of industry feedback from the informal comment period, and the need to send a quality product out to the industry to gain acceptance

of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff identifying these issues and ask for an extension for the posting of the CIP draft standards in October 2010 to be added to the schedule to develop the 010 and 011

Vote on the motion above to adopt the motion: 11 yea – 5 nay (69%)

Bob Jones suggested that the SDT is unanimous that it needs more time to do a quality job based on the industry comments, 706 directives and FERC comments. The Chair thanked the Team and suggested the Chair and Vice Chair would take this as guidance in their discussion on Friday morning with the Chair of the Standards Committee.

E. Discussion of Further Input from the Standards Committee Chair

On early Friday morning, John Lim and Phil Huff reported to the SDT on a conference with the chair of the Standards Committee, Alan Mosher. They discussed with him the time and schedule and the Standards Committee was agreeable to a 90 day extension to complete the CIP 011 work if there could be a 010 product going out to industry in July. Mr. Mosher requested the SDT create a schedule for moving forward with both 010 and 011 and suggested that in the interim between implementation of 010 and 011 that the SDT use an amended 002 to address the issue of critical assets. Phil noted they raised the remaining 706 directives and Mr. Mosher understood the difficulty getting both out by end of year but expressed the need for something by end of year if not the full package.

Member Comments on Standards Committee Call

- Confusing to throw out 010 without 011. We must be careful how we do it
- In terms of the implementation of the 010 and 011, we can’t just put out 010 and attach CIP 003-009 – effectiveness of 010 comes from 011
- The modification of 002 will include what? Not sure but looking for something to use before effective date of implementation of CIP 010 and 011. Perhaps something to give bright line of critical assets – not sure how that works well given limited time – details still need to be worked out – entities may be concerned with using one set and then implementing another soon after this.
- Disappointed that NERC and the Standards Committee don’t understand the situation. An interim change as a bridge may be another chase down a rabbit hole.
- This is essentially plan B
- The SDT needs to focus and not be distracted by political expediency – add ninety days and six more months
- We do not have to work on the 002 option – this is what they will be doing while we try to complete our work – this is the reality – while recognizing the technical difficulties – we do not work in a vacuum.
- We will be held accountable for technical shortfall pushed by politics – we need to keep 010 and 011 connected to avoid confusion.

- Keep in mind industry feedback – industry confused when 010 put out first time without support – putting medium up to high protections brings a ton of facilities and may cause further confusion if we are not careful
- We have not been assigned to amend 002 – we move forward on our own – that is a parallel path – meanwhile we get more time with ninety day extension – need to make use of that time – this team still engaged and owning its product.
- This was informal discussion with the Standards Committee Chair. He asked to come back with a formal schedule. We need to say can not meet end of year and offer an alternative that includes getting something out by end of year
- We are still operating under the original order which did not have a timeline – now the Standards Committee is imposing a timeline – this may be a fundamental change in the original charter – we will be held accountable for the final product – if they want us to meet a timeline then put it out to the public and we can react.
- We do not have to rush to get revised schedule out
- What do we do starting next Monday? What is the revised work plan? When is the next deadline for product?
- The Standards Committee has to drive this while we continue to work on CIP 010 and 011.
- We need to keep working at our pace to get job done – the short schedule proposed yesterday is not reasonable.
- That schedule is not workable nor feasible.
- We need to know if 010 is being decoupled from 011 – this is not a good idea but it does impact our work plan. Do we just guess? If decoupled and 010 has to go out in July then focus on 010 at a different pace.
- Industry said last time they wanted a whole package to react to – waste resources on splitting up – need one unit – we do the right thing – if they want something else then let them do it – we need to look back with pride on our product
- Start Monday with addressing industry comments and get to NERC by next Friday
- We need a sequencing calendar of the next few weeks leading to Pittsburgh and then to Chicago and communicate it to members soon to guide their work.
- We have comments that we need to process with requirements we have – get output to NERC for them to work with starting the end of next week for them to review – it is not the final product – hopefully by then we have more clarity on the schedule – yesterday 90 days seemed acceptable to the team.
- Plan B is not our problem, we still have charter to fill.
- Jan Bargen, FERC noted that FERC was concerned in January about splitting 002 from CIP 003-009 and industry was too. However things are different now. If 010 proceeded first, it could be filed later with CIP 011 and this also might give industry more time to consider impacts and coverage.
- Howard Gugel, NERC staff, recommended that the SDT should think of this as staggering the work vs. "decoupling." Get CIP 010 out then CIP 011 later with overlap in the comment period – also staggers the work load of responding to formal comments

– before no one knew what 011 would look like, now the industry has an idea what to anticipate now - also allows more full group review.

- Final filing does not have to be staggered and would include implementation plan – already a stagger between 010 and 011 since you have to do 010 first to then implement 011.
- I think we can move to ninety day and understand that a separate tiger team may be ready to go on CIP 002 amendment. Our team cannot provide guidance to the NERC tiger team on our draft by next week. We are not even done compiling and reviewing comments
- What if tiger team at NERC scrubs for consistency then drafts initial VSLs, measures etc. – addresses issues we discussed yesterday as a base for Sub-teams to begin addressing the comments. This can also handle the grammar and structure and work from what you have already identified.
- Won't be hard to add lines to tables – send any concepts for us to put in draft and get you started.
- Phil Huff reviewed with each of the Sub-teams where each were in summarizing the comments. Three teams are still working on summaries while others have identified key issues. None have moved on to consider how to address the comments in changes to the requirements. He noted that there was a possibility, if needed, to split up Jay Cribb's team into two sub-teams (005 and 007) and he would consult with Jay and other team members before a decision was made.
- Following the morning call with the Standards Committee leadership, the SDT chair and vice chair would schedule a SDT meeting to discuss a proposed new schedule.

III. REVIEWING INDUSTRY AND FERC COMMENTS ON CIP 010 & 011

A. Overview of Industry Input

Bob Jones reviewed the documents compiled for the SDT's review of industry comments. He summarized an overall set of results showing the percentage of support or opposition for key components and questions. *(See, Appendix #10).* Scott Mix had sent out over the weekend a "consideration of comments" document that included over 900 pages.

The Chair noted that the Team received a significant amount of input from the industry and FERC since the posting and the SDT will need to review and consider what kinds of revisions may be needed for the CIP 010 and 011 requirements based on these comments and the SDT's continuing development of the CIP. He noted that the next phase will include a pre-ballot review followed by formal ballot and underscored the point that there is a a lot of work ahead of SDT. The comment period closed on June 3 which did not give the SDT much time to review prior to the Sacramento meeting. The SDT will need to rely on and trust that Sub-Teams will work to address the comments and share with the full SDT their summary of those comments.

Member Comments

- What do the percentages actually tell us?
- One vote could represent more than one individual or company
- Many may have disagreed but only wanted to tweak one or two words
- I stressed that respondents should provide constructive suggestions. Comments like "I don't like it" doesn't carry much weight without a suggestion for improvement.
- We can say we understand their concern, address it, include it, or explain why we keep it the same.
- We will publish a summary of comments and responses.
- Can we change the responses to substantially agree with and substantially disagree with to more accurately reflect responses?
- Yes, in future comment questions we can frame it that way.
- Can we use a 4-3-2-1 next time to gauge the level of concern – we may have gotten a ton of "3's" with minor concerns instead of "disagree"
- The percentages are based on the checked boxes – not a qualitative assessment of the responses.
- I most concerned where the percentages are close to even. These are where we need to understand the concern and address them as a group.
- Physical security section may be an indication of desire to move into a separate section

- We were told not to be prescriptive but many response comments asked for more prescription to clarify.
- System security put R15-19 together – may require more work to separate out the comments per requirement – may also account for low percentages for "agree"

B. "Parking Lot" Issues Raised by the SDT in the Development of the Draft 010 and 011

The Team has maintained an ongoing "parking lot" a table list of issues raised in the course of the development and discussion of CIP 010 and 011 and as the SDT is reviewing the industry comments. These were presented and discussed by the Team and a table setting these issues out and how they were or will be resolved or handled going forward is included as an appendix to this summary *(See, Appendix #7)*

C. Review of May 27 FERC/NERC Meeting

Joe Buchierro provided the SDT with an overview of the meeting summary distributed to the SDT members (*See, Appendix #6).* John Lim noted that the atmosphere for the meeting was cordial and professional, and the meeting brought forth constructive input and ideas. In general, FERC staff agreed with the approach taken in the draft CIP-010 and CIP-011 standards, but acknowledged that a lot of work is still needed in clearly defining the requirements. Joe noted that FERC staff expressed the following issues and concerns:

- The Low impact level requirements are insufficient and need to be bolstered, i.e. the Low baseline is too low.
- The proposed 36-month review of the categorization needs to be shortened, at least for the first review cycle (possibly to 12 months).
- Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.
- The bright line thresholds stated in Attachment II need to be justified or at least explained.
- The SDT must ensure that all of the requirements are auditable.
- Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the significant effort being performed by the SDT in creating these standards. Jan Bargen, FERC, noted that they recognize the considerable amount of work of the SDT so far, but believes there is still more to be done including both the justification and baseline issues – e.g. how do you talk about the minimum, are we moving forward if more of the electric system is not covered, need to explain why is this better. There are too many items not currently included. What else is being brought in to the new standards? Is the baseline for protection of BES equipment set at the right level.

Member Comments

- **Immediate revocation.** There was also discussion of the "immediate revocation" issues – how can that be defined to allow for prompt but effective responses and which items may not rise to immediate level?
- **Low Impacts.** Is low is too low? What does that mean and how do we set it? What is the rationale?
- There is a worry that something will fall through since the low has few requirements.
- Take input and address where appropriate – do not necessarily need more requirements – FERC staff is speaking as staff, not for the commission – treat as part of the informal comment period
- Regulators are not happy with the level of coverage now. Are they asking for every asset to be covered?
- Mike Keene, FERC noted that it is not the amount of equipment but does the low have enough protection for the low equipment – some level of protection for low equipment, not just blank
- Jan Bargen, FERC, asked if there are not requirements does that mean it does not need any protection? Then the baseline may look like there is no protection where you find blanks in the tables.
- All these discussions must be couched with "in relation to what?" What are we defending against? Everything against anything?
- FERC is trying to prompt us to look at the watt levels, etc., not just the H-M-L categories – looking for measurable standards.
- Concerned about having to create lists of low for audits – need to demonstrate you have a security program rather than a site-by-site list for purposes of audits.
- We are doing something for the low categories but this may not need to be a list subject to fines – we are doing something to protect or we wouldn't be in business.
- Mike Keene, FERC, noted that policies or procedures for low impact would be a good approach.
- **Physical Security.** Things are being done for the low but the SDT may want to think about moving physical security out into its own standard. There may be no way to marry our process with adequate protection of physical assets – we have discussed this as a team but we may need to revisit.
- Question of audits for physical security – there is a level of security for those but we do not want them brought into the meticulous audit process of today – this has been a big stumbling block for many members of this team.

Bright lines

- Need to be sure the numbers we use and how we arrived at those numbers are understood by a wider audience.
- Mike Keene, FERC, noted that FERC staff wondered about the "bright line issue" that distinguished medium and high – are they in the correct spot? Not as concerned with the low.
- **Avoid the prescriptive (how).** Clarify the standard but do not be prescriptive – identify the program and what it covers – identify what needs to be covered but not necessarily "how" to cover them – must have a documented program that covers these assets.

D. Review of Dallas Workshop Process and Results

The Chair noted that this was the first time NERC has used such a workshop in the context of a standards development process and any lessons learned would be helpful for NERC to consider. He suggested there was a good industry turnout for the workshop and some excellent questions were raised and suggestions offered that the SDT should consider going forward. He expressed surprise that during the interactive open session on day that only a limited number of people stepped up. He asked what other members thought of the workshops and the following points were offered for improvements on the process:

- The highly structured questions on day one limited the interactivity.
- That is why on day two we offered an open mike session to offer the opportunity for that interaction.
- Ideally, it would have been better to have scheduled the workshop a few weeks before so that participants could process the workshop results and prepare their comments on the posting.
- Should consider allowing for break out sessions next time to encourage more interactive discussions.
- Need to think about how to clarify what are the objectives of such a workshop. Some participants may have perceived that "this was a done deal, this is how it is, and there was no need to make comments."

E. Review of the SDT's Full and Sub-Team Process for Considering Industry Comments

The Chair proposed that the Sub-teams meet to review and summarize industry comments and report back to the full SDT.

Member Comments on Proposal

- Concerned letting sub teams review comments without full group review
- Wonder if breaking into sub-teams is still doing us any good – better to look at as a full group – may be slower but addresses the overlaps with the diversity of the full group.
- Bob Jones noted the Chair's proposal is not to look at how to respond but intended to enhance the full team discussion – attempting to make the most of the limited time with the scope of the complex task. He offered as an example of the challenge of summarizing th industry comments by looking at question 9 on format since it is not part of any sub-team. *(See Section F, Format below)* and tried to provide and organize the comments by topic. This suggests that the SDT will have to go through each industry comment and 900+ pages as a full group. The full SDT will have a chance to review and provide guidance on possible revisions. This will be enhance by an initial effort to summarize and not have to repetitively review similar comments.
- Good approach –but remain bothered anytime agenda says break into groups. The schedule is wagging the dog here. We should just do the best job we can then take our lumps.

- Concerned we did not get a full chance to review in full team the sub team work before this last cycle of review.
- Splitting up work can be good and efficient, but we need to do our work prior to coming to these meetings in order to use our time together most effectively – feel like we come to class without doing our homework first
- Note that in the Version 1 SDT we also broke up to write standards but then spent hours on the phone reviewing every word of the first set of standards at the end.
- We need to spend our time here to do that and use conference calls to do homework and prepare for in person discussions
- Just as a note, we have not been able to get the "homework" done prior to the in person meeting – sub groups between meetings successful about 50% of the time – requires a level of commitment to get work done prior to coming together to create products we can use – in this case there was no time to work on prior to this meeting so we need to take some time now to do that so we can then review together – have to do the pre-processing today and tomorrow – group the comments together by topics and frequency, do not decide what to do with them yet – then use final day and a half to review as a group
- Support the ideal process of using in person time together but having to deal with the comments on short turn around as JL pointed out – we did not have enough time from close of comment period to allow for processing – in July we need to be sure we have a product ready to make the best use of in person time
- In July we may also have some initial vetting by NERC – also note there are other items that need to be added for the formal posting such as measures
- Use the sub team time now to organize comments for full group review?

F. Review of Industry Input on CIP Format (Question #9)

1. Overview of Industry Format Reponses

Bob Jones presented an overview of Industry responses for Question 9 (*See, Appendix 8)*: *Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?*

CIP 011 COMBINED REQUIREMENTS FORMAT

	Totals	***%***
Keep CIP 011-1 as one document-	(48)	40.3 %
Break CIP 011-1 into multiple standards	(38)	31.9 %
No preference-	(23)	19.3 %
Not checked -	(10)	8.4 %
Total:	**(119)**	**100**

Keep CIP 011-1 as one Document- Comment Topics
1. Better Organization and Organizational Review *(8 comments)*

2. Auditing and Multiple Violations of Single Standard. *(6 comments)*
3. Format *(2 comments)*
4. Table Format *(1 comment)*
5. Revisions *(1 comment)*
6. Alignment with Other Standards *(1 comment)*

Break up CIP 011-1 into Multiple Standards- Comment Topics

1. Retain CIP 003-009 Format *(10 comments)*
2. Audit/Enforcement/Compliance and Negative Perceptions *(9 comments)*
3. Suggested Standard Format Combinations *(8 comments)*
4. Level of Effort and Cost of Changing Format *(6 comments)*
5. Use Functional Areas *(3 comments)*
6. Consistency with Other Industry Cyber Protection Standards *(2 comments)*
7. Makes Easier Ownership Assignment and Referencing *(1 comment)*
8. Monitoring Changes *(1 comment)*
9. Aids the Revision Process *(1 comment)*
10. Focus on Security *(1 comment)*
11. Approve as a Complete Set *(1 comment)*
12. CIP Standards Should Stand Alone *(1 comment)*

No Preference or Not Checked- Comment Topics

1. Implementation, Updates and Revisions *(4 comments)*
2. Focus on Defining Auditable Requirements. *(3 comments)*
3. Reporting at a Requirement Level *(2comments)*
4. Simpler Management *(2 comments)*
5. Table Format *(1comment)*

Member Discussion of Format Comments

- The industry is even more split than the team with no strong preference for either format – suggest leaving it as proposed given the results
- Has anyone discussed with NERC anyone not liking on requirement and voting down the standard – can industry vote on the individual requirements rather than the whole standard?
- For ballot is it a vote on 11 as a whole?
- Standard 11 is an up or down – do not get to pick or choose – historically that is the way it has been done
- Historical observation – these are informal comments and not sure how much attention we got from the industry as a whole – have we had three different sets of the industry responding each time we go out – will we get a different response in a formal comment period
- So what – we have to move forward – we cannot assess whether that is true or not
- Yes, we need to move forward, but be aware of the possibility
- Have to look at the individual comments to determine if they are by a group or association versus an individual or individual company

Stu Langton reviewed with the SDT four key comments *(see below)* noting EEI and APPA represent approximately 60% of the industry. What are their arguments? Ameren suggests it will be easier to find requirements in one standard and use. EEI argued for the legacy of CIP 003-009 or at least a way similar to it as being easier for the industry to recognize and preserve sunk costs. APPA suggested sub-headings in 011 are illustrative of the need to separate into multiple standards and that multiple would be simpler to work with and revise in the future. IRC suggested functional areas with each standard being a stand-alone.

Specific Industry Trade Associations and Task Force Comments on Format

9.83	Ameren	Keep CIP-011-1 as one document	It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced. However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
9.35	EEI	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.42	APPA Task Force	Break CIP-011-1 up into multiple standards	The APPA Task Force believes the addition of sub-headings to CIP-011 is illustrative of the need to separate this standard into multiple standards. We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.
9.17	IRC Standards Review Committee	Break CIP-011-1 up into multiple standards	(i) We disagree with the current structure. We'd suggest the SDT to establish new standards by functional areas and ensure there is not a circular loop relating to other standards. Each standard should be standalone(ii) We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standards that apply generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber

			protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements? It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.

Format Discussion Comments

- What did we learn from this we did not know before? Any new gems we need to think about?
- We have to think about why people commented or not – those who commented favored splitting it up while those favoring one standard did not comment.
- Support for one over the other is not clear
- We should note that some votes may represent more than one entity, e.g. EEI, etc.
- The weight of the vote and comments are not the same – not sure the comments reflect the weight of the vote, many who support said "however, …"
- **Compliance Auditing, Enforcement and Reporting.** This hinges on the compliance reporting and whether it is done at the standard or requirement level.
- NERC will have to address it differently –
- The number of comments for each category (for against, no preference) is not relevant – if you agree, then less likely to add a comment
- This result gives us a sense the industry is not clear either. The Team needs to make the best choice for the industry then to judge. It there anything here that changes any of our minds? Issue comes down to compliance and auditing for multiple versus single standard
- NERC is still asking for clarification of the compliance/auditing issue. Did talk to compliance about the compounding issue – they said compounding is done by requirement, not by standard.
- Is compliance the same as enforcement?
- The person at NERC answering the compliance issue is with enforcement. Also talked to those in reporting about changing reporting to a requirement-by-requirement basis. There is support for this as it improves granularity of analysis.
- How does that improve organizations response?

- The perception in Congress is that cyber security is not being addressed. That perception and letting industry learn from others mistakes would be improved if reported by requirement.
- Favored single format in Atlanta – but now favor multiple standards – can we take a straw poll on where we are today. This is a structural issue we need to resolve.
- You asked the question and got industry comments – my sense the industry does not think this is worth the time we are putting into this question.
- Heard many say informally they may favor multiple standards but probably harking back to CIP 003-009. But note the SDT has already moved away from CIP 003-009.
- We asked industry what would best help them make everything secure – I did not put up a big fight before because I wanted industry to respond to the question.
- This is not a big deal to industry so let's split it and move on.
- The SDT reached a consensus decision on moving away from CIP 003-009 and then we asked industry for preference on one or multiple standards. Since last time the SDT had a clear preference for one CIP 011 and industry did have a strong preference in either direction, we should stick with the single standard
- Do not agree with that analysis. The comments, not the raw count, suggest we look again at CIP 003-009 -
- The Chair noted the SDT already voted a super majority (over 75%) to move to a new format.
- Everyone needs to review the comments in response to Question 9 before we vote on this issue.
- What does the option for multiple standards mean? We have eleven sections – would that mean eleven standards?
- Some comments suggest cramming the eleven back into the CIP 003-009 format. Need to precisely state what the two options are before we vote.
- But nothing will change between now and Friday – the split means the eleven sections we have now into eleven standards. We have already decided to move on from CIP 003-009 –
- Note that we have some new areas that may not fit into the old CIP 003-009. We are spending too much time on format.
- The SDT already voted to move forward. The debate now is how to do it – writing new content and standards now, that means industry will have to change.
- We moved away from CIP 003-009 because of version confusion – need a new set of standards – important not to fall back into the old regime.
- What was the SDT asked to do? We were not asked to rewrite everything. We were asked to take industry comments into account, not just throw it out because we had a previous vote
- If we reopen the vote then we need to look at the tables again.
- The vote to go forward with the posting was a result of months of work. I thought we all felt good about the product – the remaining concern was a minor one of format – going back to CIP 003-009 would create substantive and substantial problems.
- We asked for industry input because we did not have a super majority on the SDT to present a team proposal on the format.

- Scott Mix noted again that NERC Compliance suggested that violations are cited by requirement and not by standards.
- This is not a critical path element – lets spend the SDT's time fixing requirements – Do we need to vote on this now?
- By Friday this may become a critical path decision in order to redraft requirements for posting.
- The Chair noted the SDT's need to resolve the format issue once and for all – we left Atlanta with a super-majority but short of 75% to post CIP 011 as one standard and ask industry. The industry said we don't really care. My thinking is just leave it as one
- We may need to defer this in case we have to work on plan B stuff – not precluding making the decision later. We have the CIP 011 categories and can move forward.
- We need to look past the raw votes into the reasons one way or another offered in the comments and look at the level of concern and from what proportion of the industry – changing it is arbitrary and causes pain
- I do not conclude that someone who voted for but did not make a comment is not strong in their comment – to say we are not improving is unfair – we can move forward and maintain progress without deciding it now
- Even splitting it back into 011-021 doesn't address Dave's concern – if numbers change, it is the same concern
- While the difference in the comment votes was only 10 but some were by trade associations that may represent far more than one vote in the final analysis. Those associations seem to be on the side for multiple standards for CIP 011.

2. SDT Consideration of Single or Multiple Standard Format for CIP 011

The facilitators initially suggested first taking a straw poll on which of the two formats members favored then ask members for propose a motion on the format. The straw poll resulted in 10 members favoring multiple standards based on the eleven sections (011-021) and 9 members favoring the one standard format of CIP 011. Following this there was a motion (Doug Johnson, second by John Lim) to adopt multiple standards (011-021) resulting in 11 yeas (61%) and 7 nays (39%). The facilitators suggested revisiting this question at a later point noting the sentiment on the Team has appeared to shift in favor of multiple standards for CIP 011, but it fell short of the 75% needed to make a SDT decision on this question.

3. Standard Format Example- PCI DSS

John Van Boxtel provided an initial presentation on a possible improvement in the format displayed for the CIP. He provided an overview of PCI DSS standard format (*See Appendix 10 for the presentation slides).*

Member Comments

- Audits more programmatic rather than a specific requirement? Requires more experienced auditors.
- John is proposing we look at the format and adopt as appropriate – not asking to look at audits though PCI audits are more efficient and allows for them to look at other things – with PCI you do not get fined for everything and more focused on if you have met requirements to be recertified to process cards.
- Main differences is the measure is up in the table? (Yes) What else? (using the measurements for auditing) So it is format and content.
- Measurements would need to be substantially written different from those today sense they are the basis of the audit – like the way the guidance is built in but not the focus for audits.
- Fits with the NERC results based process puts the guidance up with the requirement and the measures in the table would be different – audit only to the requirements and not to the measures as directed by FERC.
- FERC would approve the requirement column and applicability column and not the measures column – but this puts everything in and allows us to consider what in the measures needs to be in the requirement column for purposes of audits.
- Wish we had seen this when drafting CIP 001 – given what we have in place not sure this works.
- Jan Bargen, FERC, indicated this would address much of the angst she has heard in the discussions and she like the way it integrates guidance for audits and how to meet the requirement. On the question of how it fits in current audit system, keep in mind you are creating a new paradigm and we may need to do something different on the audit side too. Integrating this into the requirement helps FERC review especially the blanks in the table – make your case for process changes.
- If FERC understood this made for one rule across regions, they may consider the change as a better approach
- It is similar to NIST approach.
- We may just need to change a few action words in the requirement to take into account the measures
- Also may address the baseline concern expressed in the FERC meeting on the 27th.
- We will work with Howard Gugel to see if it would work – think we could move forward with this format.
- Should help in drafting the requirements – clarifies and makes them more actionable and improving the auditability.
- Asking for more time – showing them this way of improving and solving the TFE and audit mess would help the argument for more time.
- Not sure but we may need to work on the question of TFE a little more to clarify how it would work.
- Should we incorporate this format going forward? Work on the requirements and let NERC staff focus on the format

- Howard Gugel– this fits in with the paradigm pursued by the vegetative standards group – there may be ways to make this work within our paradigm.

G. Sub-Team Meetings and Reports

The facilitators reviewed the process for reviewing the group reports. Stu Langton reviewed the progress to date with the SDT meeting all the deadlines and gotten industry approval to date with a very large group here, diverse, talented and bright – 38 day period to address issues – Talented basketball teams that play together the best succeed. For most part this Team has been able to achieve our 75% level for decisions. But now have less air time, need more focus and suggestions for improvement. We need to stay focused, those who like to talk may need to talk less and give more focused responses – think in terms of what we as a group need to do to get the job done.

1. Open Question (Question 54)

Phil Huff reviewed with the Team the responses to Question #54 noting we want the Team to help us be sure we have identified the right issues and determine who needs to address them. There were:

- 19 comments on clarity or wording: blank fields, several overall language improvements, and minimize use of adjectives.
- 12 comments on definitions especially hourly: move definitions to NERC glossary, appreciate local definitions, separate attachment for all local definitions.
- Timing issues – 11 comments.
- Implementation plan – 11 comments concerned about "gap" in compliance programs, sufficient time for categorization, CIP-010 may require more time.
- Categorization – 10 comments: remove low impact requirements, possible increase in risk as focus on med/low impact areas.
- Consistency – 10 comments: move requirements in the table, remove "authorship" of sub teams, requirements language referencing the table.
- Other comments on: audits and guidance, address remaining FERC directives now, access control and system boundary protection.
- Two major approaches suggested from Entergy and Progress Energy (latter regarding nuclear)

Member Questions and Comments

- Produce guidance documents – who, how and when?
- This will be done for posting by a team
- Many complained about lack of definitions where it was supplied in other area, giving all definitions in one place is a good one
- If move to multiple standards, then one glossary will be helpful

- Entergy – fully laid out approach offered for consideration – our requirements are binary, apply one or not – looking at NIST approach calls for a layered approach – also discussion of focusing resources on key risks in routable protocols.
- 853 approach may not apply to low category.
  It is not just the impact but the type of equipment that needs to be considered – we have not noted the differences between systems.
- Need to look at this for cyber vulnerability, not physical risks of natural disasters
- Did not look at scoping activities for consistency.

2. Question 53

Phil Huff provided the overview:

- 66 comments, with 57 specific comments: several referenced TFEs
- TFE comments: passwords, malicious code, appropriate use, system hardening, security event monitoring, wireless and remote address, communication and date integrity – we will need to farm several of these out to appropriate group
- Other comments: device characteristics, write clear requirements, TFE process improvements

Any comments the SDT needs to look at in particular?

- Are we going to go through each TFE requirement to make changes or considering supplying entities with flexibility? How are we going to put parameters around each requirement?
- Not all requirements are created equal. Not all requirements should be eligible for TFE though most should be – may need a black list of those not eligible for TFE
- FERC order allowed many flavors of TFEs such as legal requirements, or safety requirements, not just technical feasibility
- Directive acknowledged flexibility needed but that “business judgment” was over used – still can use or request exceptions under other categories
- Suggest not to put TFEs in specific requirements – develop a broad statement without specifying the applicable requirements
- 16 comments on passwords may suggest we need to take it up a notch and not be so granular

3. CIP 010

John Lim provided the overview of industry comments.

4. Questions 1-8, with subparts- Overall

The Sub-team in particular looked at three questions: #1 – definitions, #6 – the Attachment 1 functions, and #7 – Attachment 2 categorization of BES cyber assets.

Question 1a

1.a. BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.

34 (31%)= Agree with proposed definition
76 (69%)= Disagree with proposed definition

Dave Nortion summarized the industry comments to Question 1a:

- 71 responses were "no" with comment. Someone complained about each word in the definition
- From that created a suggested alternative definition
- Many do not think data should be there
- A definition is not "one or more" component(s) – it is just one component
- Look at systems, then components of a system, then individual items
- 11 "yes" with comments
- Separate out by operating systems suggested
- Suggestion to offer examples

SDT Member Comments and Questions

- What would be your recommendation in approach to making changes?
- Interesting observations – not sure what the implications are – first impression, we may need to make it simpler or more general or generic.
- Difficult in a definition to identify what is included in BES cyber system – have we provided enough guidance?
- Comments run the gamut of interpretation – some industry comments suggested it be "skinnied" down to just routable protocols and dial ups or it will be a monster to implement – everyone had heart burn with some word in the definition

Question 1c – control center

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

42 (40%)= Agree with proposed definition
63 (60%)= Disagree with proposed definition

- 23 pages – 63 disagreed, 40 agreed and many with no preference still had a comment.
- Control center should have "two or more" of the functions listed ("not one or more" functions)
- "…this standard is not the correct place to redefine BES and any language that does will force a no vote …"
- Some wanted definition of control centers
- "Multiple locations" mean geographic locations or multiple generating units?
- EEI comment: suggested a new definition
- Another comment attempted to scale down the scope of the requirement
- Does "location" refer to physical or electrical(?) locations?
- Generation plants refer to power plant or generation facility?
- Control center a cyber asset or a physical location?
- Remove AGC systems from function 1?
- Suggestion that in bullet 3 "asset management" may not be appropriate and should not be included
- Suggestion to remove bullet 4 as redundant.
- Bullet 5 comments suggest removing it
- Some real nuggets in the 23 pages we need to mine to improve the definition overall

Member Comments

- On restoration as not a cyber function – much of the communication system for manually switching needs to be considered from transmission center point of view.
- High level coordination has to occur to make sure it is safe and secure.

Question 6:
CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.
62 (58%)= Agree
45 (42%)= Disagree

Jim Fletcher presented a summary of the industry responses:

- 58% agree
- The one issue dominated the comments – the attachments needs more definition, examples and guidance in attachment 1
- Next better definition of real-time and the 15 minute window
- One suggestion to use 30 minutes but that seems beyond "real-time"

Summary data (slashes indicate repeat comments)
____ – "condition" not correct in context
No – use 30 minutes to match EOP std
No – Attachment 1 clarity, needs guidance //////

No – Attachment 1 should be guidance, not part of the standard /
No – "communications" implies voice
No – avoid using undefined terms or redefining preexisting NERC terms
No – when does the 15 minute period commence //
Yes – situational awareness of current state of bes results in too broad a scope ////
Yes – "functions" of Attachment 1 confusing overlap and ambiguous //////
Yes - need cut out for nuclear facilities covered by NRC
Yes – "shutdown condition" definition
Yes – concern for 15 minute window and real time adverse impact //
Yes – mitigation of event within 15 minute window needs to be included
Yes – voltage control needs to reference bes voltage
Yes – inter-entity communication too broad could include signal paths covered by other standards /
Yes – boundary for without external assistance /
Yes – need specific examples for reliability functions ////////////
Yes – delete attachment /
Yes – real time definition needed /
Yes – monitoring and control too broad
Yes – substitute NERC adequate level of reliability document for attachment 2
Yes – need to refer to other document for system restoration functions rather than make a definition here
Yes – remove 15 minute window /
Yes – treat control and monitoring as separate functions ////
Yes – inter-entity communications could imply voice
Yes remove inter-entity communications unless BES cyber systems can be defined to include components from multiple entities
Yes – system restoration is not a function supporting reliable operation
Yes – remove attachment 1
Yes – include more definition of functions supporting reliability of the bes in standard
Yes – should explicitly exclude voice systems

SDT Member Comments

- In terms of reliability determination something is lost in scoping – need to look at subject from the reliability coordinators perspective

Question 7 Attachment II

Question 7: CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

72 (67%)= Agree with proposed definition
35 (33%)= Disagree with proposed definition

Rod Hardiman presented a summary of the industry responses including the following points:

- If look at question then more accurate to note as much as 75% actually disagree
- Blackstart is not high impact/only include units in regional plan/openly include primary blackstart units – 24 comments

- “must run” is inappropriate term – 12 comments, 5 more related
- Should have a “no impact” level below low – 10 comments, 5 more related
- Provide justification for thresholds/thresholds are arbitrary – 10 comments
- Categorization should be based on engineering studie/need waivers from thresholds -9 comments
- Define “primary cranking path” – 9 comments
- Questions about defining “transmission line”, local area , transmission facility, etc.
- Sorted attachment 2 categories by the number of times commented on

SDT Member Comments

- Top three deal with generation and transmission support centers –
- Some called for combining the generation categories, as well as the transmission categories
- Comments on 1.14 and 1.13? RAs and TOPs running at less than high given their coordination and communication? If interconnected, should all, even small ones be considered “high” to establish high trust levels?
- There is a level of protection at the application level but hard to put into the standard here
- Important to have some sort of protection from injection attacks – have some level of data protection – appropriate that industry pushes forward to get vendors to produce product

Other issues in 010

- Requirement R3 for updating lists and categorization – have not had a chance to review comments, assume many significant comments and will need to review in the next call – Question 5
- Variable generation is important to wind and solar providers and how it fits

5. Governance, Change Management, System Lifecycle and Information Protection and Maintenance Sub-Team

Dave Revill introduced the Sub-teams work noting it covered Questions 11, and 40-48.

SECURITY GOVERNANCE AND POLICY Question 11 – R1

11. Requirement R1 of draft CIP-011-1 states, “Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:” and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

58(56%)=	**Agree with proposed definition**
46(44%)=	**Disagree with proposed definition**

John Stanford presented an overview of industry comments:

- Seeking clarity in the list, policy phraseology, or definitions of terms (19)

–Examples include: Formal, annually, boundary protection, sanitization, security roles and responsibilities, authorized access, personnel, third-party, non-employees, addresses.
–Desire to have terms used in later requirements defined here

- Seeking clarity in the policy expectations, purpose or structure (11)
  –Desire to have all access related issues defined here
  –Numerous questions on what is meant by policy language
  –Several concerns about how to demonstrate compliance with a policy
- Concerns about the term “annually” (9)
  –Numerous suggestions on alternate wording for clarity
- Questions about Senior Manager (8)
  –Mostly delegation or approval concerns, possible conflict with R3, or claims of double jeopardy between R1 and other requirements
- Concerns about burden of proof, compliance, legal or ownership (4)
  –Several concerns about allowing for non-ownership or non-operation of BES Cyber Systems
  –A few raised contractual obligation concerns
- Concerns about policy being too prescriptive (5)
  –Seems to be confusion about general policy hierarchy
- Suggested edits without actual disagreement (4)
  –All over the map
- Generic references, non-substantive comments, or misplaced (3)
  –Examples include comments about change management or “ditto” and “me too” comments submitted by others on other requirements

SDT Discussion Comments

- Need to be clearer on the overall intent here
- Some may be looking at results based requirements – looking for the what rather than the how
- Many comments want to clarity about what you are asking – clearly getting mixed message of clarity on what is expected versus being too prescriptive
- Would a guidance document help here?
- The phraseology may be asking for a lexicon – how far do we want to go there?
- Maybe there are some things we can glean from the responses to clarify the language rather than saying we need to teach them what we mean
- Some interpretations may need to be left to legal but others are terms of art that we may need to clarify with purpose of our intent
- Some concern about why governance and policy structure is a regulated area
- This is a balance between binary requirements and a policy structure
- Reinforcing the value of policy in a good security program
- FERC looking for management responsibility and policy is a linchpin
- Complying with the controls may not be enough – need good policy to drive compliance
- If done right policy can set a good foundation
- “annually” was mentioned here and in other groups – needs to be addressed

6. BES Cyber System Maintenance (R26) Question 47, R26

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

41 (48%)=	**Agree with proposed definition**
45 (52%)=	**Disagree with proposed definition**

Dave Revill presented the following overview of industry comments:

- Concerns about the interaction between the list of personnel in 26.1 and the lists granting authorized electronic and physical access (13)
- Concerns about the interaction with other user/account management requirements (12)
- Comments regarding the allowance for emergency maintenance situations (2)
- Requirements on maintenance devices should include system hardening (2)
- All maintenance devices should be documented in a list (2)
- Ensure that systems used for maintenance do not act as an unauthorized access point (1)

He noted they also got comments on the definition of “maintenance” – some said to consider the temporary connection also have appropriate controls.

SDT Comments

- Overlap on responsibilities that we may need to address
- Some entities may not have specific devices set aside for maintenance – but may be burdensome the random use of a laptop to perform maintenance
- What is “maintenance”? What are the devices are you connecting for maintenance activities, such as field devices
- In guidance document may want to put in something about how you can provide evidence of compliance with this requirement

7. Electronic Access Control (R7 –R14)

Question 17. Requirement R7 of draft CIP-011-1 states “Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.” Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

56 (58%)=	**Agree with proposed definition**
40 (42%)=	**Disagree with proposed definition**

Sharon Edwards presented the following summary of industry comments:

- Misunderstand that they are to define acceptable use
- Local definition/description of account types
- Soft language
- Top themes:
- 1 - Need a strategy for designing baselines by impact levels – we missed the mark
- Strategy going forward include policy requirements, verification of implementation
- 2 – revocation of access – do not like the time parameters for revocation, transferred personnel should not be treated as risk, and clarify when the clock starts for no longer needing the access
- make distinction between "primary" access and "secondary" access; primary access includes the domain user account, remote access credentials, and physical access; etc.
- 3 – clarity and definitions on acceptable use, account types, system access, remote access, external connectivity, wireless, etc.
- 4 – separate remote and wireless access
- 5 - consistency
- 6 – quarterly review is excessive
- Discussion – if we take this approach it needs to be justified and segmented appropriately in h-m-l

SDT Questions or comments

- Don't make distinction between BA, TO, TOP, GO? Those are the comments? That is surprising in terms of the parameters for revocation.
- Comments may be coming from control centers who want to relax the requirement – this is in contrast to the request to make it "immediate."
- May need to segregate requirements and make distinction for those terminated for cause and others who are lower risk
- Are we addressing privileged accounts? This is a case were you need to run, not walk.
- Yes, but it is not under revocation
- Need to coordinate revocation ahead of termination of those with key access
- Highly recommend not using "primary" or "secondary" access – you either have access or don't – need a three level recognition of revocation including those with privileged accounts
- "quarterly review" – assumption the this included quarterly reauthorization – that would be a burden – need to clarify quarterly reauthorization is not part of the requirement
- need to coordinate the timing required in other requirements
- need to look for overlaps and need for coordination between the teams
- quarterly review is part of the monitoring, not reauthorization – need to clarify proposal
- quarterly review is meant to catch and fix those we missed – should not have to self report those.

8. Response and Recovery

Cyber Security Incident Response (R27 –R29)

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

54 (61%)=	**Agree with proposed definition**
34 (39%)=	**Disagree with proposed definition**

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

52 (60%)=	**Agree with proposed definition**
34 (40%)=	**Disagree with proposed definition**

BES Cyber System Recovery (R30 –R32)

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

39 (46%)=	**Agree with proposed definition**
46 (54%)=	**Disagree with proposed definition**

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

52 (65%)=	**Agree with proposed definition**
28 (35%)=	**Disagree with proposed definition**

Scott Rosenberg presented the overview of industry comments:

- Guidance on cyber security incident classification highlighted.
- Definitions
- Coordination with 001
- Incident response for low impact or non routable connections should be removed?
- Consistency between requirements related to impact level?
- Single versus multiple incident response plans and testing issues.
- Combine incident response testing and review/update.
- Review results of incident response tests in other than 60 days
- Recovery testing
- Recover plan testing clarifications
- Data retention identification requirements of personnel responsible
- Coordination of physical aspects of cyber security incidents
- Incident response and recovery plan reviews and question around changes required
- Suggestions for re-wording

- Coordination of backup plans

SDT Questions or comments

- FERC said we may not have enough requirements? More important to set a base line, focus on quality not quantity with security need in mind – not the number of requirements but the right ones
- Timing questions – can NERC develop a Gant chart of the timing requirements?
- Summarized in one place would be helpful to entities
- Good appendix to a guidance document
- Helpful to team for coordinating and consistency across the requirements
- A table of all the timings? Yes
- “annual” is across several requirements – may need a joint effort to define a common understanding
- Proposing the team draft glossary definition of “annual”?
- Careful – this may become an audit issue – may need to be given to the Standards Committee.
- Define for local purposes – how does the team want to use the word? Do we mean 365 days? Once a calendar year?
- When we use time related items, need to identify what we are trying to achieve – think about a flexible window for compliance and auditing.
- Any time based requirements? Quarterly?
- Good to have a base line approach to incident response.
- Need to present context without putting into requirements
- Taking requirements and putting into a table? Are there requirements for how to do that from NERC?
- Industry has said it makes sense and offered suggestions for refinement – may need to identify multiple requirements in the same table or split them out
- Can we put up an example of a table for comparison? Send out by email then take a look at together tomorrow.
- Backup control center – some asked why do I need to do anything else?
- Might put in words to say fully function backup center is sufficient for recovery
- Still need a recovery plan.
- This is a cyber incident possibility – a hot backup may be corrupted or could lose both – cold backup is less likely to be corrupted in the same incident.
- Business continuity to keep operating and then there is restoration of the original assets
- This is recovery of the cyber system – not a backup system
- Need to recovery ability to execute control – differs from recovery of the assets
- Three levels: recover capability, recover the assets, and recover.
- Purpose to protect the grid or the assets?

9. Systems Security (R15 –R19)

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

25 (27%)=	**Agree with proposed definition**
67 (73%)=	**Disagree with proposed definition**

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

40 (45%)=	**Agree with proposed definition**
49 (55%)=	**Disagree with proposed definition**

BOUNDARY PROTECTION (R20 –R22)

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

28 (31%)=	**Agree with proposed definition**
62 (69%)=	**Disagree with proposed definition**

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

49 (56%)=	**Agree with proposed definition**
38 (44%)=	**Disagree with proposed definition**

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

38 (46%)=	**Agree with proposed definition**
44 (54%)=	**Disagree with proposed definition**

Jay Cribb noted that the industry responses to Questions 35-39 covered more than 100 pages.

R15 – Malware Prevention

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

37(40%)=	**Agree with proposed definition**
56(60%)=	**Disagree with proposed definition**

Jay Cribb summarized the industry responses as:

- Don't' require malware testing
- Very difficult to audit current language
- Need device class language or many TFEs

SDT Comments and Questions

- What is the problem with malware testing?
- Language looks like you are ask to put malware into your system to test the system
- Need to clarify we are trying to prevent propagation of malicious malware
- Testing has to take place outside the production system
- Testing the protection systems
- Test in a real world already – we know the products work – why test my antivirus when it is tested every day in the real world –
- need to clarify the language and intent
- do we need this here or is it already covered elsewhere?

R16 – Patch Management

- What starts the clock? Release vs. availability
- Fixed date of implementation

SDT Comments and Questions:

- Getting reliability tested on their systems first and certifying it is more important than the contract.
- #2 is a misnomer – the requirment asks for applying the patch and pick a date or date for mitigation – reasonable requirement –

R17 – system hardening

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

37(41%)=	**Agree with proposed definition**
54(59%)=	**Disagree with proposed definition**

Jay Cribb provided the following overiew of Question 17 industry responses:

- What is "externally accessible physical port"? (By far the most common comment)
- Physical port disabling on devices that are already secured

SDT Comments and Questions:

- Physical ports? Need to relook at this – reframe to cover accidental use
- Need to disable the local services too
- We test many best practices that do not actually add to security

R18 – security event logging and monitoring

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

66 (69%)=	**Agree with proposed definition**
30 (31%)=	**Disagree with proposed definition**

Jay Cribb provided the following overview of Question 18 industry responses:

- Is weekly manual log review really needed with continuous monitoring?
- What is a "cyber security event"?

SDT Comments and Questions:

- None.

R19 – data and communications integrity

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

74(80%)=	**Agree with proposed definition**
19(20%)=	**Disagree with proposed definition**

SDT Comments and Questions:

- Very unclear what is validation and what is satisfactory?
- True validation happens at the application layer – dependent on vendor, etc.
- Proving malicious intent of invalid data received is very problematic (impossible)

Boundary Protection

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

45 (48%)=	**Agree with proposed definition**
48 (52%)=	**Disagree with proposed definition**

Jay Cribb provided the following overview of the industry comments:

- Rename this and the tables back to ESP
- Remove or clarify the alerting timeframes (the 48/12 hrs)
- Weekly review of log entries
- Clarity – what is a "communication path", "authorized access"
- Clarify access points and their interaction with multiple BES cyber systems

SDT Comments and Questions:

- Looking at taking review of logs and alerting time frames and moving them up into the requirement – thus one requirement for system monitoring rather than in two places
- Pull physical into it too?
- Did we have a question that asked if prefer consolidated or separated?

- Comments favored keeping physical and electronic separate
- But is it the same distinction for monitoring?
- Makes sense
- But caution – physical and electronic monitoring may be done by two different sets of people – careful how it is worded

R21 – system boundary

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

50 (55%)= Agree with proposed definition

41 (45%)= Disagree with proposed definition

Jay Cribb provided the following overview of the industry comments:

- Remove the requirement – overly prescriptive
- How does this requirement differ from R20

SDT Comments and Questions:

- Is it realistic to address and incorporate the changes suggested by this July?
- These are just the top issues from 100's
- Little more detail on system boundary – is it about the logical separation piece?
- R21 separates systems that could have a single point more than they are now – it is not just systems boundary
- Confusion about the differences between the two, some argued to combine
- Making it a requirement may be too much – putting in a best practice and making it auditable
- Point is to address shared systems and being sure they are protected to the same level – or not share – if combine the two we can achieve the same goal and reduce confusion
- Access points can be physical or electronic – need to clarify to improve understanding
- Access point is the interface and that is what you need to protect – not the same as the firewall
- Focus on the interface
- Making distinction between firewall challenge and access control(?)?
- Requirement addressed access control at the interface level

R22 – Protective systems

22. FERC has mandated 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. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

27 (29%)=	**Agree with proposed definition**
67 (71%)=	**Disagree with proposed definition**

Jay Cribb provided the following overview of the industry comments:

- Remove and put the systems in scope of the relevant requirements
- Weaker than the current standard

Jay Cribb then noted some overall issues raised in the industry comments:

1) TFE allowances – where and how. All of our requirements will need them
2) Clarity around when the requirement applies to "systems" and "components"
3) External connectivity matters – do not require external connectivity in order to meet RQ's
4) "no impact" category needed

SDT Comments and Questions:

- approval rating for this section very low for this whole section
- many of the comments related to the existing requirements and concerns
- can we retool these requirements in 38 days?
- Doesn't need more people but need to retool timing by asking FERC to give NERC more time – need to retool the time – I think the FERC people understand, but do the NERC people – change the time
- NERC can ask for more time
- Take up and address the timing issue tomorrow as part of the schedule discussion

10. Personnel & Physical Security

Doug Johnson presented the summary of industry comments on personnel and physical security. The one on training we changed the least from the CIP garnered the most comments.

- Questions 12-14 for R2, 3 and 4
- Questions 15-16 for R5 and 6

PERSONNEL TRAINING, AWARENESS, AND RISK ASSESSMENT (R2 –R4)

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

23(23%)=	**Agree with proposed definition**
77(77%)=	**Disagree with proposed definition**

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

59(60%)=	**Agree with proposed definition**
39(40%)=	**Disagree with proposed definition**

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

43(47%)=	**Agree with proposed definition**
48(53%)=	**Disagree with proposed definition**

Doug Johnson presented an overview of industry comments on Question 12, R2

- What security awareness program is being referenced? (see R1)
- Replace the term "reinforcement" with "awareness material and replace "provide all" with "make available to all"

SDT Comments and Questions:

- May want to divide R1 much the way others divided into the other requirements
- What should the policy or program have in it? R1 says must have a policy
- R1 language could be adjusted to be consistent with the following – may break 1.4 into multiple parts – R1 lacks detail
- Does programmatic guidance need to be in R1 or broken out into sub parts? Approach affects other areas too
- Need to write it down and come back to for more discussion – how is the low approach depicted and approached?

R3

- 3.2 – add clarification or make it role specific
    - (the clarification is important to acknowledge that the intent is clearly not to have all personnel with electronic access to any BES cyber system to become network engineers)
- What is Annual?
- Would it be better to include the table for consistency?

STD Questions and Comments:

- "annual" appears in only one place – in R1
- here the concern is about any time frame – not the specific word
- need a consistent way to reference to be clear
- at least once every twelve months – is that not clear enough?

R4

- Why is photo ID now being required?
- Address how to better handle vendors and contactors

STD Questions and Comments:

- Not realistic to require CISCO to go through training process for remote access
- Concern about allowing third party access and support especially in an emergency to maintain reliability
- May need NERC to certify and support a third party vendor training
- Entity may need to define and document emergency situation – allow for exception in such circumstances

- Not something NERC creates – need to put into a requirement – unless willing to do that, then NERC is not going to do it – operator stuff was created by the industry – NERC will not certify appropriate persons with operator access
- Distinction is in the authorization for access control – person given temporary access working through someone with authorization – latter is required to document and have management approval
- Operator certification is provided by third parties
- NERC could not provide training for the procedures for all of the entities, especially given the diversity of entities and their procedure
- Focus here is on remote support access
- Escorted remote access? No equivalent on electronic side to the current escorted physical access – an issue for all the entities
- R3 and 4 have exception clauses for emergency to the training requirement – some better definition in the maintenance that documents the emergency clause rather than a requirement for training in emergency situation

R5

- Immediate revocation of access
- What is meant by the term monitor?

STD Questions and Comments:

- Is escorted electronic access an open issue for interpretation?
- That is not the interpretation requested
- “authorized access” is not used in the standard – the standard does not address the concept – only unauthorized physical access and granting electronic access are in the standard
- parking lot issue of combining physical and electronic access revocation – 80% of those offering comments agreed to separating the two?
- Need a single person revocation of both physical and electronic access – personnel revocation
- Are we moving forward with them as separate items? Yes
- Granting access and revocation need to be consistent

R6

- Physical Access Control Systems need to be defined
- Potential for a fourth column

STD Questions and Comments:

- Consider a fourth column where needed to where physical controls need to be applied – we do not need physical access controls lumped in with the electronic controls – do we need a fourth column?
- For end user it may be better to have a separate requirement rather than search through all of the related requirements
- Comments suggested embedding electronic controls – but keep physical controls separate

- There is a broader category here – requirements apply to BES and protective systems
- Keep physical access on their own
- Parking lot issue: protection requirements for electronic and physical access controls and systems (Phil Huff)
- May need to insert a "local" definition

Overall question for SDT

- Is it possible for an entity to have no BES Cyber Systems?

STD Questions and Comments:

- May want to address in 010
- Several hundred distribution providers who do not have BES assets but need target protection

IV. OTHER 706 ISSUES AND CIP DOCUMENT PREPARATION

A. FERC Order 706 Issues In Addition to CIP 010 and 011

On Thursday the Team took up how to address 706 issues that have been termed "post Version 4 issues" that include:

A. Access Control Redundancy/~~Defense in Depth~~ (two or more diverse security measures in constructing electronic and physical security perimeter)
B. Active vulnerability assessments every three years
C. Forensic data collection

SDT Members Discussion

- Issues raised during the workshop
- Comments also appeared in question 54 and in Doug Johnson's group
- These are non trivial and will take even more time and discussion than taken so far – trying to get 011 done first without delay.
- Willing to write single page description of each issue?
- Strong concern in industry about punting to another version – can we address in a limited manner at least as a place holder – concerned it is doomed with FERC without defense in depth for example – scope it down and phase in.
- That is not what the FERC directive said.
- Yes will take time, but is this justification for an extension from FERC.
- Rename defense in depth to access control redundancy of access perimeters
- Need to do vulnerability assessments on redundant not live systems – careful how we write – also need clarification from FERC (Mike Peters) on the issue
- Not talking about putting in two access points to perimeters
- Peters said defense in depth is fundamental and bolting on later will cause trouble for industry

- Need more two way communication as to what FERC is asking for, the intent of the request. This is too important to make assumptions and the goals are too important/
- Put in words from the actual order – paragraph 480
- Paragraph 502 also says flexibility – it also says it is not intended to create an inflexible requirement.
- Misconception written into the order – most systems already have three levels – can do three things at the same level rather than pick different levels.
- Ignore the Commission's request and tell them what they should have said
- Seeking clarification
- Paragraph 725 – need to pull out of 011? – Paragraph 710 requires data in blackout report and improved forensics.
- We need to research what the commission is asking for.
- Jan Bargen, FERC, noted her understanding is that you do not have cyber security if it is not in depth – too severe an interpretation that it has to be all or nothing and cannot been done in pieces – you can explain progress and point to in the requirements and note what else needs to be worked on – recognize you are working on a new paradigm and have a window of opportunity.
- Language in 706 says you have flexibility in how to approach concerns – by accepting phased approach to implementation in the past FERC is indicating you can apply to defense in depth and forensics.
- Putting so much protection at the boundary that you need some depth – if get through firewall you need another layer – not necessarily another duplicative firewall but cannot get through just one vulnerability.
- These don't have to be next to each other.
- We have to assume the bad guys are in your business system and you need to protect the high end assets.
- We will need to review current draft requirements to see what is already addressed, then assess what it would take to address in part or full the issues.
- Support that approach – also agree we are in a new paradigm – also need optics we are trying to deal with issues – and fourth, we need clear grounds for an extension.
- Fourth issue of operation test of the recovery plan addressed in CIP 011
- Need to review and develop possible ways to address in small team groups.
- Under forensics – half may already be dealt with under Jay's group and the rest in Scott's under recovery.
- Can we ask Carnegie-Mellon to help with this – meeting is in Pittsburgh next month
- We have now have 38 days left – Jay's sub-team is not done and it is the key – we need a backup plan – we just added to Jay's sub-team's responsibility – have to figure out how to address this soon or have a backup plan – maybe it is just a patch of the old CIP 005 and 007 and not a brand new system?
- Item B will also be addressed in Jay's group

- Item A, part 2 in my group – have not discussed yet – given volume of comments to deal with, not sure if we can get to it in the time frame we have
- We are in a countdown mode with an artificial deadline. In order to get it right, we may need to adjust the deadline

B. Implementation Plan Options

Scott Mix presented the implementation plan concepts and approach.

- Open issue about early compliance – example, implementation time frame that adds up 2 or 3 years before version 4 kicks in but buying new EMS now and want to be compliant with v4 in the new system - legal said “no” – hopefully they did understand the question, will try to discuss issue with legal further.
- Floated to FERC the concept of compliance with high in two years, medium in five years and low in ten years – focus on smaller number of assets first with the biggest bang for the buck or investment of time and resources.
- What about entity with only low assets? Do they get to wait eight years to do anything? How can we incentivize them to move quicker or start earlier?
- Implementation plan may look similar to a mitigation plan – come up with list of assets “quickly” (30-90 days?) – create an implementation plan for your entity – provide guidance and oversight with yes or no on the early compliance plan and audit to the accepted plan – regional entities are the ones who approve the plan
- May create confusion for audit teams and regions
- Cannot let industry appear to be delaying the inevitable
- Favorable reception by FERC staff for early compliance plans – at least one of the regions is considering a similar approach – proposal may still need time and attention
- Nuclear process is a similar approach
- Have a team to help draft approach

SDT Questions and Comments

- Flabbergasted – if going after highs in the first phase
- Jan Bergen, FERC, noted that it is worth exploring opportunities to implement sooner than 10 years.
- Mike Keene, FERC, suggested this function as long as requirements in 011 are done in appropriate manner – conception is an acceptable approach
- Focus on the real attack surface first – we don’t have the proper focus on the appropriate attack surface – too focused on big iron and not the cyber system.
- The approach makes sense – especially for those putting in new systems now – concern from some that they do not want to have to comply with two different versions at the same time
- I am not a fan of approach – letting entities build their own plan misses the interdependence of the small and big entities – do not think one entity gets fined on a low

asset down the road from another entity that is not under compliance for anther four years – also end up with different timelines for compliance on physical protections

- Have to order the sequence of implementation – cannot do everything at once.
- Have to run a test on the low to be sure of impact before full implementation.
- Allows for quicker implementation of those easier or lower cost without waiting.
- Take care of controls in the tables to address connectivity since they were removed from 010 – where applicable
- Concerned about overhead and oversight and approval from regions – subject to subjectivity – every entity plan will have to be processed by the region
- What to demonstrate we are moving forward – if set a future date, any delay waiting for that date makes it look like industry is not forward – better to show some in industry are moving forward and not waiting.
- Disappointed that proposal offered to FERC without discussing with sub-group or full team – be careful not to introduce complexity – advantages to letting entities to move forward but danger of adding complexity – better to give industry reasonable firm times in which to comply – need to be less concerned about when low impact entities comply and focus on the high
- Scott Mix did not bring up the plan at FERC meeting– Alan Mosher did.
- Some of the “lows” have access to higher assets through IP.
- Need to file an implementation plan ready for time of posting.
- Need to start drafting soon – need direction on how to proceed.
- Is it based on a fixed date per requirement per impact or flexible date with submission of implementation plans for approval by regions?
- Come back with a formal proposal for members to express a preference.

On Thursday, Scott Mix offer the following Implementation Plan options for the SDT’s consideration:

1. **Multiple fixed dates (based on connectivity and dependent on impact level)**
   4 -6 3 -8 2 -5 1 -0= **58 (3.2 of 4)**

2. **Entity-specific implementation plan**
   a. need to develop boundaries and approval guidance
   b. resource issues at regions for approving plans
   c. multiple versions in play at the same time for audits
   d. will require “true-up” of CIP 011 requirements for connectivity, etc.
   e. consistent with current NGP plans
   4 -3 3 -11 2 -4 1 -1= **54 (2.8 of 4)**

3. **Single fixed date (independent of impact level)**
   4 -4 3 -9 2 -3 1 -2=**51 (2.8 of 4)**

4. **Fixed date for each requirement, for each impact level**

a. some requirements would be the same for all levels
b. may have issues with "early compliance
c. will require a separate plan for NGP

4 -0 3 -1 2 -14 1 -4= **35 (1.8 of 4)**

SDT Questions and Comments:

- #4 – when do I need to be in compliance? I cannot give you a date, not to mention the inconsistency of being in compliance with one element before another
- Only alternative is reduce the number of dates and gloom them together – getting it done early may be detrimental – should improve reliability by allowing early compliance
- Cyber system and cyber system components are different – suppose to be looking at functions –
- This is a complex system with many components – I apply patches to individual components
- For nuclear plants – are they allowed to beyond the recommended date? Why is it an either or choice here? Is there a hybrid? Some fixed dates under #2
- Some might be fixed date but other programs may lend themselves to early implementation.
- Option 2 is more successful in nuclear arena – scope is more focused – with electric industry looking at vastly larger and more diverse set
- Favor a set date – option #3 – fixed and singular independent of impact level
- SE – difference between requirements makes for a nightmare for implementation under option #4. Option #2 may work well for entities with multiple business units
- multiple fixed dates based on connectivity and dependent on impact level as option 1
- Option 2 is based on entity registration

C. Low Impact Baseline

- Do we need to modify something in the governance section to identify low to better depict what is included in low?
- Put everything up in R1 but detail in the subsequent requirements – hard to follow – if R1 is the baseline, it only looks like an outline and needs more – Sub teams need to know how to proceed
- Sounds risky to go off and just assume it will be dealt with in R1.
- Sub teams would need to identify and shift words up to R1.
- Clarifies next steps for sub teams.
- Do we need to revisit decision to shove everything up to R1 and governance? Better to put baseline in the individual areas to tailor to the need.
- R1 doesn't have the detail needed – need the detail in the individual areas
- Jan Bargen, FERC, noted the format presentation by John Van Boxtel would offer you the opportunity to identify the detail you need in each section.
- Articulate the baseline in the table for each section?
- References in the technical controls are not tied back to R1.

- Controls do not appear to be well fleshed out at this time in current form putting everything up in R1.
- The requirements themselves are the policy – go through and identify those that need more clarity and lift them up to a table in R1.
- Should we address connectivity with low?
- Not addressing levels, applies to H-M-L – concern is to protect from upstream.
- If have a routable connection it should be higher – substations connected to control center or control system – it is the connectivity we are trying to protect, not the individual substation.
- John Van Boxtel's presentation allowed for recognizing that connectivity.
- Everything to date has focused on BES assets – paradigm shift to look at the connectivity – if routable connection to substation, it should not raise the level of every relay in the substation.
- It is the level of protection on the low item needs to be higher if it is connected – but only for certain requirements.
- Taking it down into the individual areas and put into our requirements, not sending it over to move into R1.
- Agree, but don't need policy in every requirement – do not need to write new policy requirements.

V. NEXT STEPS AND ASSIGNMENTS

Following the Sacramento meeting it was agreed there would be a need for weekly sub-team meetings and possible sub-team leads meetings. Later in June the schedule would be adjusted to reflect this and include some SDT meetings to develop drafts for NERC staff to review in advance of the July meeting in Pittsburgh.

The Chair suggested convening the SDT to review a new draft schedule the following week once more information was available from NERC and the Standards Committee.The Chair thanked Kevin Sherlin for his excellent support for the SDT in hosting this meeting.
The meeting adjourned at 11:00 p.m. on Friday, June 11, 2010

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 23rd Meeting Agenda
June 8, 2010, Tuesday- 8:00 AM to 5:00 PM PDT
June 9, 2010 Wednesday- 8:00 AM to 5:00 PM PDT
June 10, 2010 Thursday- 8:00 AM to 5:00 PM PDT
June 11, 2010 Friday- 8:00 AM to 12:00 PM PDT
Sacramento, California

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

Proposed Meeting Objectives/Outcomes:

- To review the CSO 706 SDT 2010 Work plan and Schedule;
- To review and adopt CSO 706 SDT 2010 Consensus Procedures draft;
- To receive updates on other related cyber security initiatives;
- To review the results of the FERC/NERC May 27 Meeting;
- To review the results of the May 19-20 Dallas Technical Workshop;
- To review the documents to be produced for the July, 2010 CIP posting;
- To receive an overview of the industry informal comments on CIP 010 and 011;
- To review industry input on the CIP format and to test SDT consensus on CIP format going forward;
- Sub-teams review industry input from the Technical Workshop and informal comments and propose any potential changes in the draft standards;
- SDT reviews Sub-Team reports on industry input from workshop and informal comments and any proposed changes in the draft standards;
- To review progress on the Implementation Plan Drafting Group and the Guidance Document Drafting Group; and
- To agree on next steps and assignments

Draft Agenda

Tuesday, June 8, 2010 8:00 a.m.-5:00 p.m.

- Introduction, welcome and opening remarks
- Discussion of CSO 706 SDT Work plan and schedule: June-December, 2010- *Stu Langton*
- Review and seek agreement on Drafting Team Proposal for refining the SDT Consensus Procedures
- Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

- Review results of the May 27, 2010 NERC/SDT Meeting with FERC and guidance for sub-teams
- Review Technical Workshop overview and results
- Initial Overview of Industry Response to Request for Informal Comments
- Review of industry input on CIP format and consensus testing on CIP format going forward
- Sub-Teams meet to review and discuss industry comments *(Afternoon)*

Wednesday, June 9, 2010 8:00 a.m.-5:00 p.m.

- Sub-Team Meetings, Cont'd *(till mid-day)*
- Sub-Team Reports and SDT Discussion- Key Issues, Comments and Possible Changes to Requirements. *(Afternoon)*

Thursday, June 10, 2010, 8:00 a.m.-5:00 p.m.

- Sub-Team Reports and SDT Discussion- Key Issues, Comments and Possible Changes to Requirements

Friday, June 11, 2010, 8:00 a.m.-12:00 p.m.

- Review Next Steps and Sub-Team Schedule and Production of new Draft Requirements and related filing documents.
- Review the SDT Pittsburgh Meeting Agenda and Perform the Meeting Evaluation
- Review Implementation Plan Drafting Team progress and next steps
- Review Guidance Document Drafting Team progress and next steps

Appendix # 2 Attendees List
June 8-11, 2010, Sacramento CA

Attending in Person — SDT Members and Staff

1. Jim Brenton	ERCOT
2. Jay S. Cribb	Southern Company Services
3.Joe Doetzl	Kansas City Pwr. & Light Co (T/W/Th)
4. Sharon Edwards	Duke Energy (T/W/Th)
5.Gerald S. Freese	America Electric Pwr. (T/W/Th)
6. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation (W/T/Fr)
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Patricio Leon	Southern California Edison
10. John Lim, Chair	Consolidated Edison Co. NY
11. David Norton	Entergy (T/W/Th)
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy (T/W/Th)
14. Kevin Sherlin	Sacramento Municipal Utility District (W)
15. Jonathan Stanford	Bonneville Power Administration
16.Tom Stevenson	Constellation (W/Th/F)
17.Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
18. John Van Boxtel	WECC (T/W/Th)
19. John D. Varnell	Technology Director, Tenaska Power Services Co.
Scott Mix	NERC
Roger Lampila	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

Rob Antonishen	Ontario Power Generation (T/W)
Jackie Collett	Manitoba Hydro (W/Th/F)
Frank Kim	Hydro One Networks Inc. (Th/F)
Rich Kinas	Orlando Utilities Commission (T)

SDT Members Not Participating

William Winters	Arizona Public Service, Inc.

Others Attending in Person

Jan Bargen	FERC
Summer Esquerre	Next Era Energy (FPL)
Jim Fletcher	American Electric Power
Joel Garmon	Next Era Energy (FPL)
Michael Keane	FERC
Jerry Mercado	SMUD
Sam Merrell	CERT/Software Engineering Institute
Brian Newell	American Electric Power
Guy Zito	NPCC

Others Attending via Readytalk and Phone

June 8, 2010, Tuesday

Annette	Johnston	Mid American Energy
Justin	Kelly	FERC
Peter	Kuebeck	FERC
Drew	Kittey	FERC
Jerome	Farquharson	Burns McDonald
Daniel	Bogle	FERC
Ingrid	Rayo	Constellation
Rod	Hardiman	Southern Company
Bill	Glynn	Westarenergy
Steve	Newman	Mid American Energy

June 9, 2010, Wednesday

Rod	Hardiman	Southern Company
Ingrid	Rayo	Constellation Energy
Jerome	Farquharson	Burns McDonald
Peter	Kuebeck	FERC

June 10, 2010, Thursday

Drew	Kittey	FERC
Peter	kuebeck	FERC
Rod	Hardiman	Southern Company
Justin	Kelly	FERC
Jerome	Farquharson	Burns & McDonald
Ingrid	Rayo	Constellation Energy

June 11, 2010

Ingrid	Rayo	Constellation Energy
Rod	Hardiman	Southern Company
Annette	Johnston	Mid American Energy

Appendix #3 NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

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

III. Activities That Are Permitted

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

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

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

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

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

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

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

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

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

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
4/12/2010	**SDT Meeting Atlanta, GA (Southern Co) (4/13-16)**	**Present Controls draft for full SDT review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
4/19/2010	4/19-4/23/2010 4/23/2010	**SDT Sub-Teams and Leads Meet to Finalize Documents NERC Receives and Prepares Full Package for Industry Comment**
4/26/2010	**4/26/2010 4/27/2010 4/28/2010 4/29/2010**	**SDT Sub-Teams Develop Package SDT Reviews with NERC Staff Proposals SDT Scoping Meeting on Documents SDT Reviews and Approves Full Package for 30-day Industry Comment Period**
5/3/2010	**5/4/2010**	**Informal Comment Posting for full package starts Completes on 6/3/2010**
5/10/2010	**SDT Meeting Dallas, TX (Luminant) (5/11-13)**	**Review Parking Lot Issues, Prepare for Industry Workshop and Begin Development of Guidance Documents**
5/17/2010	5/19 & 5/20/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
5/24/2010	5/24 to 5/28/2010 5/27/2010	**SDT Considers Comments from Workshop Meeting with FERC Staff to Review Draft Standards and Posting**
5/31/2010	6/3/2010 6/4/2010	**Informal comment period ends SDT Reviews Comments Received Sub team meetings to Review Comments Received**
6/7/2010	6/7/2010 **SDT Meeting**, **Sacramento, CA (SMUD) (6/8-11)**	**Sub team meetings to Review Comments Received Industry comment review, response process, re-drafting, as needed**
6/14/2010		Sub team meetings to prepare sections for review

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
6/21/2010	SDT Meeting and Subteams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review
6/28/2010	SDT Meeting and Subteams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review
7/5/2010	NERC Staff review	Sub teams complete all work assignments & NERC Review
7/12/2010	**SDT Meeting, Pittsburgh, PA (CERT) (7/13-16)**	**Finalize & Approve Documents for posting for 45 day formal comment period**
7/19/2010	7/19/2010 7/21/2010 7/21/2010	**-NERC seeks SC Approval for Ballot -Post CIP Standards for Formal Comment -45 Day formal comment period begins (closes on 9/3/2010) -Begin Ballot Pool Formation**
7/26/2010		**Formal comment period for CIP standards Prepare for industry webinar**
8/2/2010		**Formal comment period for CIP standards Prepare for industry webinar**
8/9/2010	**SDT Meeting, Chicago, IL (ComEd) (8/10-13)**	**Formal comment period for CIP standards Finalize presentation for industry webinar**
8/16/2010	8/17/2010 8/19/2010	**Hold Industry Webinar (tentative) Ballot Pool Formation Ends**
8/23/2010	8/25/2010	**Initial Ballot Begins**
8/30/2010	9/3/2010	**Initial Ballot Ends**
9/6/2010	**SDT Meeting Winnipeg, Canada (Manitoba Hydro) (9/7-10)**	**Review ballot results Respond to comments received Draft revisions to standards**
9/13/2010		Sub-team meetings
9/20/2010	9/20/2010	Sub-team meetings, NERC Staff Review

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
	9/24/2010	Full SDT on-line meeting to approve revised draft of documents for re-ballot
9/27/2010	9/27 to 10/6/2010	Re-Ballot Period
10/4/2010	10/6/2010	Re-Ballot ends; comments received by SDT
10/11/2010	**SDT Meeting, Toronto, Canada (OPG) (10/12-15)**	**Prepare responses to 2nd ballot comments**
10/18/2010		**Sub-teams meet to adjust requirements, as needed**
10/25/2010	10/25/2010 10/29/2010	**-Prepare and finalize revisions to standards** **-NERC Staff review** **-SDT Approval for re-ballot (if needed)**
11/1/2010	11/1 to 11/10/2010	3rd Ballot Period (if needed)
11/8/2010	11/10/2010	Ballot period ends
11/15/2010	**SDT Meeting, Baltimore, MD (Constellation Energy) (11/16-19)**	**Prepare responses to 3rd Ballot comments**
11/22/2010		*NERC and SDT finalize responses to ballot package*
11/29/2010		*Seek SC and BOT Approval for Filing*
12/6/2010		*Seek SC and BOT Approval for Filing*
12/13/2010	**SDT Meeting** **Tampa, FL** **(FRCC)** **(12/13-17)**	**SDT Meeting to review Filing** **Completion of Phase 2**
12/24/2010		***Submit for Regulatory Approval***

Appendix #5 SDT Consensus Procedures

CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM

Proposed Refined Consensus Guidelines (June, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing a Team consensus on substantive issues which the industry will need to approve by a 2/3's vote.

~~***Postings for Industry Comment.*** *For decisions on CIP standards documents to be posted for industry comment where the Team finds that 75% acceptance or support is not achievable but an option or options under consideration had greater than 50% support from the Team, the Team's accompanying Comment form will seek industry input to help the Team resolve any differences and select an option going forward.*~~

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least ~~*4*~~ 12 hours after the time of the announcement).

2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 75% super-majority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

Appendix #6- FERC Meeting Summary May 27, 2010

Cyber Security Order 706 SDT — Project 2008-06
SDT Meeting with FERC Staff and Industry Stakeholders
May 27, 2010 Meeting Summary
FERC's Offices
Washington, DC
Joe Bucciero

Meeting Executive Summary

Atmosphere was cordial and professional, and the meeting was constructive.

FERC staff agreed with the approach taken in the draft CIP-010 and CIP-011 standards, but acknowledged that a lot of work is still needed in clearly defining the requirements.

FERC staff expressed concern that the Low impact level requirements are insufficient and need to be bolstered. The Low baseline is too low.

The proposed 36-month review of the categorization needs to be shortened, at least for the first review cycle (possibly to 12 months)

Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.

The bright line thresholds stated in Attachment II need to be justified or at least explained.

The SDT must ensure that all of the requirements are auditable.

Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the monumental effort being performed by the SDT in creating these standards.

Cyber Security Order 706 SDT — Project 2008-06
SDT Meeting with FERC Staff and Industry Stakeholders
May 27, 2010 Meeting Summary
FERC's Offices
Washington, DC

Joe Bucciero

1. Introductions and Anti-Trust Guidelines

Regis Binder, FERC, welcomed the NERC SDT members, industry stakeholders, and other participants to the meeting and covered meeting logistics. Joe 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.

John Lim, SDT Chair, thanked FERC for hosting the meeting and providing the meeting room and facilities. He also reviewed the proposed meeting agenda.
FERC staff stated that they are not speaking for the Commission, and they recognize the importance of the cyber security issues to the industry and the country. FERC staff recognized the magnitude of the herculean effort and the excellent hard work being done by the SDT, in addition to everyone's day jobs, and stated this effort was fully appreciated.
The proposed agenda for the meeting is included as an attachment to this meeting summary. FERC staff was encouraged to ask questions throughout the presentation/discussion offered by the SDT regarding the new draft CIP standards.

2. Review of CIP-010-1

John Lim reviewed the strategy, approach, and history of CIP-010-1. The primary objectives of this standard are to: (1) help scope the electric system assets that are within the purview of the CIP-010 and CIP-011 standards; and (2) establish a list of reliability functions and "bright-lines" for categorization of the BES cyber systems.

a. Discussion of Scope

The process and criteria currently being used today for identifying critical assets in the electric system are thought to be inadequate. For example, less than 5% of the existing generation facilities around the country are considered to be critical assets, so the SDT has identified a new approach in the new CIP-010-1 standard.
The scoping process in the existing CIP-002 standard calls for identification of critical bulk electric system assets, then the associated critical cyber assets. In CIP-010, there are no 'out of scope' bulk electric system assets; instead a categorized list of those assets and their related cyber systems is required. That is one of the major differences between CIP-002 and CIP-010.

Attachment I of the draft CIP-010 standard is meant to provide the definition of scope and applicability. CIP-010 requires the categorization of cyber systems by defining a list of the real-time reliability functions that could have an impact on the reliable operation of the bulk electric system, and if a cyber system is doing any of those functions, then it is within scope.

Categorization of the electric system assets and the cyber systems based on multiple levels (High/Medium/Low) of their potential impact on the reliable operation of the bulk electric system is key aspect of the new draft CIP-010 & CIP-011 standards.

Attachment II of the draft CIP-010 standard is meant to provide the criteria or “bright lines” to identify the potential impact (High/Medium/Low) on the reliable operation of the bulk electric system if the electric system asset or its cyber systems are destroyed, degraded, misused, or otherwise rendered unavailable. The concept is to take a more holistic view and move away from consideration of individual critical cyber asset issues, and place more focus on ‘system’ impacts.

One of the significant concepts behind collapsing the CIP-003 to CIP-009 standards into a single standard was to clarify the requirements for audit purposes and reduce the incumbent paper work thereby providing focus on the security of the key cyber systems. The SDT is concerned about the auditability of the requirements, and wants to ensure that the CIP-010 and CIP-011 requirements are auditable.

b. Discussion of Response Time

The CIP-010 requirements apply to cyber systems that are relevant to real-time operations (not long term planning or systems that do engineering or marketing). The current benchmark parameter is “impactful within 15 minutes”, where the 15 minutes relates to when the incident occurs. Discussion and feedback from the industry to determine if the 15 minute parameter is appropriate has been solicited through the recent informal posting and comment form for the draft CIP-010 and CIP-011 standards.

c. Discussion of Bright Lines

Question: In CIP-010 R1, the phrase “execute or enable” is used; what is meant by enable?

> In some cases, a cyber system directly performs a function (as identified in Attachment I), but in other cases (e.g., data collection/aggregation or display) it is providing information to an operator or other systems to enable functions.

Staff observation: Once these draft CIP standards are filed, they will create a different benchmark or situation from the existing CIP standards for the industry to consider. Are we improving or not? What is the key yard stick? There seems to be a general belief that the number of assets identified to be critical to reliable operation of the BES under CIP-002 is inadequate (i.e., not enough assets being identified, less than 5% of generation). When these new draft CIP standards are filed, how can it be demonstrated

that the key assets are identified? The size of unit is not the necessarily the key. Is the “medium” level of impact adequate for the number of units that can potentially fall into that category?
The intent is for the new CIP-010 standard to be comprehensive, in that all bulk electric system and cyber system assets will be covered to some level of impact. The “bright lines” are being provided to help clarify the assignment of the appropriate level of impact to each of the BES Cyber System assets. The SDT recognizes that measuring impact against what is considered ‘critical’ today is not good enough since today’s results are not acceptable.
The SDT is looking for guidance from all industry participants with a stake in the game as to what is acceptable for the bright lines, and hoping to receive some guidance through the informal comments from the industry.

Allen Mosher: The draft CIP-010 standard is an improvement over what we have today, and we need to implement it soon. It’s difficult to compare it to what we have today, because we have a different paradigm. We want to maximize our effort to identify the most critical assets and focus on the control systems. We should worry most about common use failures and wide spread loss of the bulk electric system.

Gerry Adamski: What are the criteria for identifying if an approach is adequate? What is adequate, and how do we identify it to help tweak the product? A thoughtful dialogue may be needed to better define the “bright lines” in Attachment II.
While the number of megawatts or the size of a unit can be one of the criteria used, the impact on day-to-day operations is also very important. The SDT should have a solid basis for the numbers used in Attachment II to define the “bright lines” that are used in the draft CIP-010 standard.

For example, generators, units, plants, etc. that are used intermittently, are they single or multiple control systems? The number of generation MWs connected to assets or to the control systems? If three units combined are over 2000 is it a High impact system? Are three separate control systems that are networked together a single cyber system? How does contingency analysis factor into the impact level criteria evaluation, if at all?
It might be helpful if the SDT can quantify the number of MWs of generation that would be classified as High impact using the new draft CIP-010 standard vs. today under the CIP-002 standard.

A re-ordering the “bright lines” criteria identified in Attachment II should be considered, putting the control center criteria first.

FERC expressed concern that the requirements applicable to the Low impact criteria are not sufficient, and that the Low/Medium impact bright line is set too high.
Throughout CIP-010 there are references to quantities of MW; how were those quantities selected? Adding insight into how the values were determined (e.g., was a study done; is it from operating experience) would be very helpful. NERC indicated

that many of the bright-line values came from a variety of resources available to NERC, plus active participation and input from OC & PC members in the development of the standards. FERC does not have a magic study to use in its review and assessment of the bright lines.

d. Discussion of Guidance and Auditing

The SDT members agree that guidance is necessary for each of the requirements. There hasn't been enough time spent to-date to fully develop or flesh out guidance on each requirement.
There is reason to believe not everyone knows or can identify all the key assets that auditors are concerned about, since the auditors learn something new every time they perform an audit.
Two NERC auditors have been engaged with the process of defining these new draft CIP 010 & CIP-011 standards as well as participation from the regional entities. There were many auditors involved in last week's SDT technical workshop held in Dallas, TX.
The easiest standard to audit is a checklist, but that is the worst way to audit.
Transparency is needed on how an entity is audited. The entity needs to know how the audit will be approached. In the filing, a summary description of what discretion is left to the entity may be helpful.
NERC will have its audit department staff review the draft CIP standards and provide comments from an auditor's perspective. Are the "bright lines" bright enough?

e. Discussion of Compliance Review Schedule

The draft CIP-010 R3 requires at least a 36 month review cycle, since the bulk electric system doesn't change that much that often. Currently a three year process is used by the entities as a review trigger for going back to look at the standards and consider if any changes have occurred that would impact the High/Medium/Low categorizations. What are the triggering events for this review? Possibly the SDT should consider that a one to two year review cycle is needed at first, and then followed by the traditional three year cycle.
How assets are allowed to move from one category to another over time may be critical. Where should these requirements be addressed; in the audit process? Also, do we need to address assets that may be critical to a neighboring entity but may not be critical to my entity even though my entity controls the assets?

3. Review of CIP 011-1

Phil Huff provided an overview of CIP-011 and led the discussion. The overall approach by the SDT was to combine CIP-003 through CIP-009 into one standard, taking into account the FERC directives, the SDT's review of the DHS catalogue of cyber security requirements, and incorporation of those requirements that would be beneficial to the reliability of the BES.

a. Discussion of One vs. Multiple Standards

CIP-011 is viewed as one standard with many parts, and as such putting all of the requirements together in one standard would tend to minimize the possibilities for multiple violations of the same standard, and the number of violations in general. Retaining the multiple standards approach would tend to make synchronization of the requirements and versioning of the multiple standards more difficult, resulting in possible multiple reporting of violations for the same standard. Retaining the multiple standards approach would possibly make it easier for entities to split up the CIP requirements for implementation and monitoring in a way to match the unique organization of the entities.

The SDT is divided on the issue of format for CIP-011 – putting in one standard communicates the standards should be seen as one – multiple standards makes it easier to change individual standards, separately, but creates the compliance issue of potentially multiple violations across multiple standards for the same identified problem. The single standard approach would simplify the ability to incrementally change the full standard. On the other hand, given the way violations are reported now, one standard may result in this standard standing out like a sore thumb if it combines so many requirements.

The SDT wanted to ask the question regarding format of the CIP-011 standard to gain some industry feedback, since the SDT itself could not reach a super majority decision on the best format approach. The SDT wants industry feedback on the approach, including if it makes sense.

b. Discussion of the Requirement Tables

A new feature in CIP-011 is how the requirements are presented, which is based on applicability/impact on the reliable operation of the BES. There are several subject areas identified in CIP-011, including: security governance and policy; personnel training, awareness, and risk assessment; physical security; electronic access control; etc. Each requirement has several characteristics identified, and each requirement is assigned to one of the subject areas. A requirement is represented in the CIP-011 draft standard through a table that groups together all of the requirement's characteristics.

A few questions were raised by FERC staff regarding the requirements tables in CIP-011. For example, what is the intent of the 'blank' entries in a table? Are entities required to do anything? Can an entity be found in violation of a requirement if the corresponding table entry is blank? Should entities look at the rows in a table to determine compliance with the requirement?

c. Discussion of Specific Requirements and Wording

CIP-011 R1.3: What is the intent? The requirement to clearly identify a senior senior manager is not really stated in the requirement. The requirement is for the entities to designate a single official. How do you determine that, and when do you have to designate this individual? Nothing specifically says an entity shall designate this individual.

The training requirements seem to be scattered around the CIP-011 draft standard. Possibly a consolidation of the training requirements would be helpful. Also the choice and use of words such as 'training' vs. 'education', vs. 'credentials' needs to be reviewed for consistency of meaning. What is 'sufficient' training? Need to include a sense of frequency and magnitude around the training requirements.

Overall, the SDT needs to review the draft CIP standards with respect to the use of adjectives (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability. For example, R5 vs. R16/R18 states "ensuring" vs. "guaranteeing". Which one is correct?

The SDT acknowledged that this draft of CIP-011 was prepared by multiple subteams within the SDT, and the multiple teams did not always use consistent language in developing the requirements. The SDT has been focused on developing compliance elements, but is now focused on writing the requirements clearly while also minimizing the need for TFEs.

d. Form and Format Issues

The Enforcement office at NERC is looking at the draft CIP standards with respect to the needs for enforceability and compliance, as well as the table structure of requirements. CIP 011 covers the requirements previously included in CIP-003 thru 009; have these requirements been incorporated or do the requirements from CIP-003 thru CIP-009 need to be maintained?

Some of the more document-focused requirements are no longer in the new draft standards. Does that meet the equally protective criteria? The intent is to improve the standards by removing the administrative requirements that do not improve reliability in any way.

The need for more than paper evidence of compliance may lead to actual need to demonstrate compliance. For example, current requirements call for paper demonstration rather than allow for actual demonstration of the protection system; the latter improves security. Creation of paper lists of authorized personnel is a Chinese fire drill that does not improve system security.

A mapping will be done to identify gaps in the standards that we will address in the version coming out in July for industry comment and ballot. The idea is to explain clearly why the gaps are there, and that these gaps do not affect the reliability of the BES.

One of the biggest issues is the perception of a culture of compliance. Now you have multiple violations of the same standard, and from the way it would be reported today, it would stick out. NERC/FERC need to make sure this does not present a skewed view of the CIP standards.

Concern was raised about the status of the components that make-up the tables. The 'R' (for requirement) is not used for the components in the table. How does that relate

to the roll-up methodology; what is and is not a requirement? What is the status of the actual wording in the parent requirement (ahead of the table), and how does it relate to the components in the table?
In Tables R4 to R9, there seems to be a general formula for the requirement, which is each responsible entity shall apply the criteria with a goal of preventing unauthorized access to BES cyber systems. However, a responsible entity that has a Low impact BES cyber system does not have an entry in the table that indicates that the entity has to address any of the subcomponents. Is that entity still subject to the requirements of R5? Similarly, if a Medium impact cyber system has in fact restricted physical access according to 5.1, but there is in fact an unauthorized access – would that be a violation of R5? The intent of the entries in the tables and the requirements needs to be clarified. How will the goal of preventing unauthorized access be accomplished on assets with Low impact, when there is no requirement defined?

e. Discussion of Applicable Time Barometer

The discussion centered around why was a 15 minute time period was selected as the barometer for the impact time stated in the draft CIP-010 standard. Isn't it dependent on current system conditions? Whatever time period is chosen will it be readily evident to the entities?
How quickly can it be determined that there is an impact on the bulk electric system? When does the impact happen? Is it objective enough for an entity to determine for purposes of verifying for audits?
Is a qualifier needed for peak electric system conditions or most stressful conditions? Time of year and load conditions may impact the determination of the time used.
The draft CIP standard is written around how the set of functions impact the reliable operation of the bulk electric system; some functions have more immediate impacts and others take longer to impact the BES.
Misuse of a system may have a longer lead time, far longer than fifteen minutes, but an equally devastating impact.
The SDT might need to revisit the definition or application of the fifteen minute time period.

4. Implementation Plan

Scott Mix provided a high level overview of the implementation plan concepts and issues being considered by the SDT. A subgroup has been formed to prepare the text for the Implementation Plan. They will likely start meeting during the SDT Meeting in June 2010 in Sacramento.
Scott Mix presented the slides he recently gave at the SDT Workshop in Dallas, TX. He noted that the plan is to retire CIP 002 and CIP 003-009 within a transition period as CIP-010 and CIP-011 become effective.

a. Discussion of Implementation Plan Issues

The SDT is working on relevant timetables for implementation of the draft CIP-010 and CIP-011 standards, including how to prioritize the effort in terms of importance and in terms of timing.

The SDT needs to try to identify in a general sense which assets will eventually fall into each of the High/Medium/Low impact categories and how many assets will be in each category. A significant benchmark between the CIP-002 and the CIP-010 & CIP-011 standards will be the number of assets involved, and has that number increased in size and scope.

How should the industry be incentivize to implement the new CIP-010 & CIP-011 standards, but not the Medium or Low impact controls at the expense of first focusing on the High impact assets. Possibly a 'rolling' implementation of the standards is in order. What is the impact categorization of a BES cyber system if it moves up or down an impact level? How should it be considered in the implementation plan?
The Implementation Plan subteam will also work with the nuclear folks to discuss policies and impacts vs. an implementation schedule. Two stakeholders from the nuclear industry will be part of the implementation plan subteam.

Some level of reporting to FERC on implementation plan development (including content and schedule) is encouraged. The reporting should be designed to provide review of justifications, milestones, and accountability while offering a degree of oversight.
One possible scenario for implementation plan development would be for the entities to quickly develop their lists of categorized assets, immediately followed by the establishment of their respective implementation plan. The responsible entities should then report their implementation plans to the respective regional entity for approval. Guidance documents will be prepared by the SDT to provide a level of consistency and assistance in the development of the implementation plans. Potential conflicts between compliance deadlines and audit schedules must also be considered.
Allow entities to be compliant early especially through implementation of system upgrades that will need to be compliant later. We'll need to recognize that some entities may need additional time to do the job right while maintaining appropriate levels of oversight. For example, larger organizations may have a larger portion of assets affected by the new standards.

b. Discussion of Transition and Migration

A transition plan from the existing CIP-002 to CIP-009 requirements to the new draft CIP-010 and CIP-011 requirements is needed. Some CIP-011 requirements are a direct replacement for those in CIP-003-009 and a migration plan should be developed for those, while other requirements are new and an implementation plan is needed. Plans to guide the entity may be helpful to both the entity and the auditors.

A roadmap for the transition/migration activities would help in the development of a schedule to accomplish these tasks.

The draft CIP-011 standard does not appear to provide a significant base level of protection for the low and medium impact controls. FERC expressed concern that the controls requirements for the "low" impact systems do not provide an adequate level of protection. The blank entries in the tables in CIP-011 might imply that there are no control requirements.

c. Discussion of Physical Controls

Physical items or locations may have protection but may not be auditable as a NERC standard, which focuses on cyber assets. For example, substations have physical protection, but how can an auditor be convinced that the physical fence or padlock was there thirty days ago.

The focus of the SDT is on cyber security. The team considered a separate SAR for physical security. The issue is not when the fence went up, but was it secured and was the lock actually locked – actually visiting remotes sites to prove this might be too much.

Too much energy goes into such audits without corresponding benefit of protecting the system. An auditor might randomly select a few remote sites – because selection is random, but an entity would need to protect them all.

d. Discussion of Immediate Revocation

It's questionable if the industry can meet targets for "immediate revocation of access". Do timeframes of 72 hours work?

May need a primary and secondary revocation applied to remote and/or physical access – this will also depend on the "cause" for revocation.

What does "immediate" really mean in these cases? For example, an entity may need to revoke access of an individual before letting the person go for cause.

"Immediate" is not auditable, even if we set a time period. "As soon as possible" would be a better phrase or a set time period would be sufficient. If it is a planned termination, then it can be immediate because it precedes the termination. If it is part of an emergency, revocation may need a reasonable time period.

e. Discussion of Security Systems Protection

FERC suggested adding a fourth column to the tables in CIP-011 that would list the physical/cyber security system protection required for each asset. The intent is to apply

the appropriate level of security. It was also suggested that a function be added to the table in Attachment I of CIP-010 for security/protection systems.
Security systems impact the BES

Passwords – maximize use without being prescriptive – suggested language – cut down on TFE's

f. Beyond CIP-010 and CIP-011

FERC Order 706 included some directives (e.g., defense in depth) that have not been addressed so far. There was too little time to accomplish these requirements and it might have derailed the process to this point.
Concern is that some of the items may have been part of the paradigm shift FERC was asking for in Order 706. How can some of these items in the order be defined, or implemented, or audited, etc.?
Implementation of an active vulnerability assessment (testing) can be contrary to reliability and security. Special care and guidelines are needed for this requirement.
The December 2010 date for filing of the new draft CIP standards for approval by FERC is not one of the Commission directives. It can become an informational filing, since it is not making law, and may be changed with FERC approval. Need to implement improvements sooner, but may not be able to resolve issues now.
The SDT is planning to file the new draft CIP-010 and CIP-011 standards by December 2010, and will start in January 2011 to look at the other remaining issues – may be a continuously moving target.
Think about how to telegraph the issue to the industry
The recent SDT Technical Workshop was aimed in part at telegraphing this schedule to the industry and thereby telling them the new standards are not a completed deal.
'Defense in depth' is implementation of guidance or guidelines for layered security, that is guidance for designing but not necessarily an auditable requirement.
The SDT would benefit from a shared dialogue with FERC Staff on this and other issues about what we are trying to achieve, the overall objective, and what is needed for the industry to reach it. This dialogue would go beyond just the standards, but could also cover how you approach audits and compliance.
NERC and the SDT still have to legally deal with the directives in FERC Order 706, and ask for clarification in the December 2010 filing. The SDT may ask for clarification of specific parking lot issues, or maybe a separate filing on those issues should be developed.

5. Closing

The dialogue and sharing of information during this meeting was constructive and has been very useful.

The FERC staff reminded us that they do not speak for the Commission. They may not agree with the statements or agreements reached. However, with continued dialogue and progress on the issues we may at least achieve a mutual understanding of the problems and concerns being addressed.

Gerry Adamski asked FERC staff about their general sense of acceptability of the body of work to date? Also, what needs more work?

> The approach is responsive, but as discussed earlier, there are many questions remaining, including how the impact levels will be applied. There is still a lot of work to be done to achieve the filing by the end of 2010. It is an ambitious schedule, but there is recognition of the quality and amount of effort involved.

Meeting adjourned.

Appendix #7 "Parking Lot Issues"

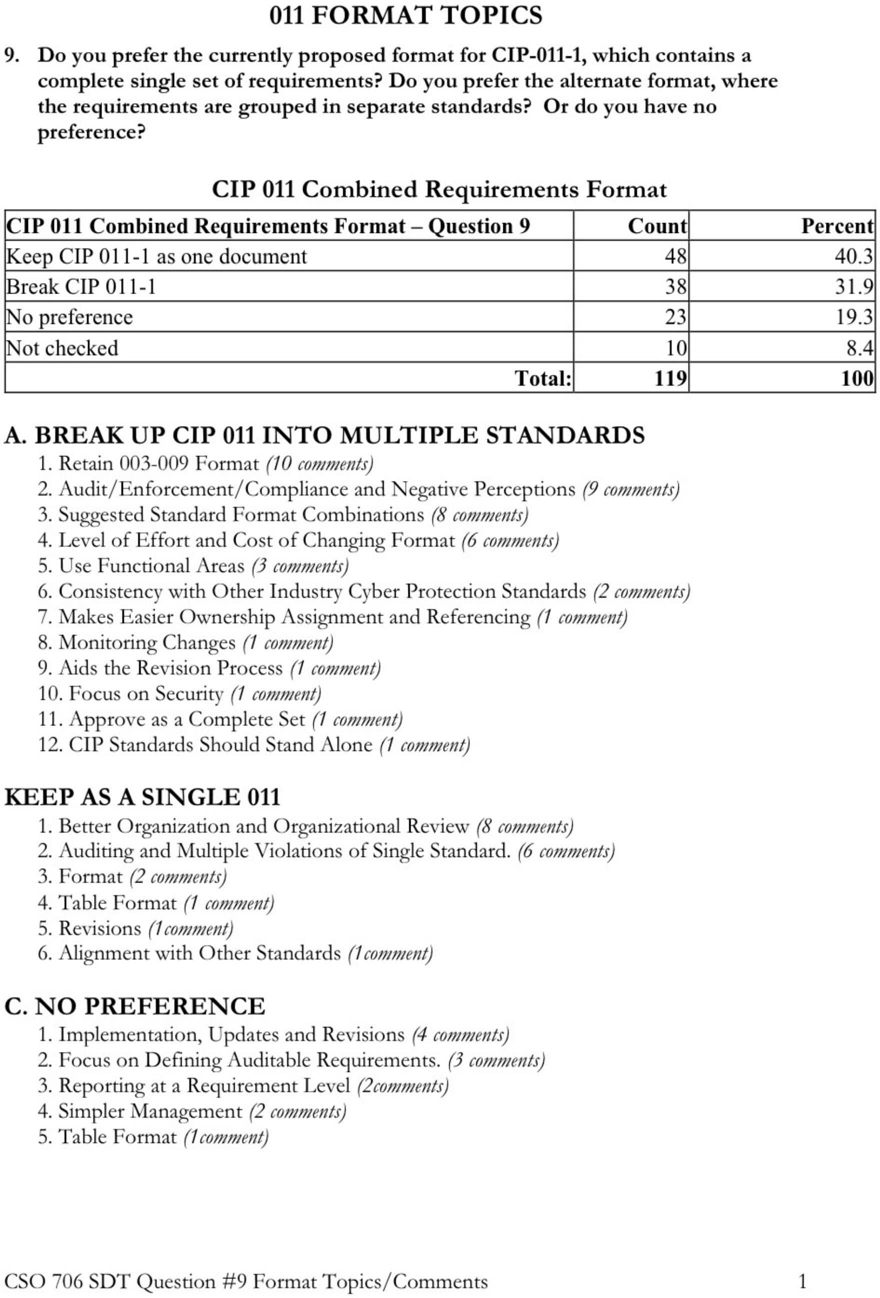
CIP VERSION 4 PARKING LOT (JUNE, 2010)

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
Review clarity of item 1.1, Attachment 2 – Generation Facilities and criteria for Contingency Reserve and Reserve Sharing	Rich Kinas	4/29	CIP-002	**AI:** Revise item 1.1 with input from the industry through the informal comments received.
Shouldn't there be delegations made by the Senior Manager for any exceptions (CIP-011 R2 & R3)	Jackie Collett	4/29	Governance	**Resolved** by the revised CIP-011 text that was posted.
User type access (R3) 3.2 Review the need for network device training (Operators, etc.)	Jim Brenton	4/29	Physical/Cyber & Access Control	Possibly regarding the level of access for outward facing and inward facing devices. What type of user training is required for each level? **Add role-based access (e.g., admin vs. application level access) – physical access & training requirements. Awareness training for everyone, and role-based training as required.**
Combine tables for electronic and physical access control systems (R6, R20, & R22)	Philip Huff	4/29	Physical and System Security	**AI:** Double-check that the proper requirements are incorporated in the respective tables.
Remove ~~Training~~ Termination for physical	Doug	4/29	Physical	

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
access to Low Impact (R9)	Johnson			
What do the blank cells mean in the tables in instances where a timeframe is given? (R9)	Jackie Collette	4/29	Howard Gugel	Do they mean there is no requirement at that particular level? **AI:** Double-check the table entries to ensure that the entries are indicative of the requirement. Possibly a statement should be added to the Guidance Document that describes what is meant by a blank entry in a table.
Monitoring the baseline configuration means monitoring the physical location as written. (R23)	Rob Antonishen	4/29	Change Management (Dave Revill)	**AI:** Is baseline the right term? What do we mean by changing physical location?
What timeframe for issuing alerts (Table entry 18.2)	Jackie Collett	4/29	System Security	**AI:** What is the response time requirement? In what timeframe should the alerts be issued?
Need to address what disciplinary actions are? Should physical or cyber access be revoked?	Jackie Collett	5/11	Disciplinary actions (physical/cyber access)	AI:
Combine the revocation of physical and electronic access requirements (including remote access) into one topical area of the standard	Phil Huff	5/11/2010	Personnel access (Sharon Edwards)	**AI:** Need to investigate possible alternatives. Have a requirement to develop a procedure for handling

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
				revocation of access.
Review “objective” statements to ensure they do not implicate requirements	FERC	5/27/2010	All	
Make requirements text consistent throughout the Standard	FERC	5/27/2010	All	
Global review of adjectives like “sufficient”, “appropriate”, etc.	FERC	5/27/2010	All	
Baseline for Low level of Impact	Drafting Teams	6/10/2010	ALL	**Completed on 6/10/2010**
Description of Timing (e.g., annual, months, etc.)	Howard	6/10/2010	NERC	
Protection requirements for electronic and physical access control systems	Doug/Phil	6/10/2010	ALL	
Broad Application of TFE Statement	SDT	6/9/2010	ALL	
Gantt Chart for Compliance Deadlines	Varnell	6/9/2010	Howard	
Exclusion for Entities that don’t own cyber systems	Doug	6/10/2010	Full SDT	

Appendix #8 Overview of Format Comments



011 FORMAT TOPICS

9. Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?

CIP 011 Combined Requirements Format

CIP 011 Combined Requirements Format – Question 9	Count	Percent
Keep CIP 011-1 as one document	48	40.3
Break CIP 011-1	38	31.9
No preference	23	19.3
Not checked	10	8.4
Total:	**119**	**100**

A. BREAK UP CIP 011 INTO MULTIPLE STANDARDS

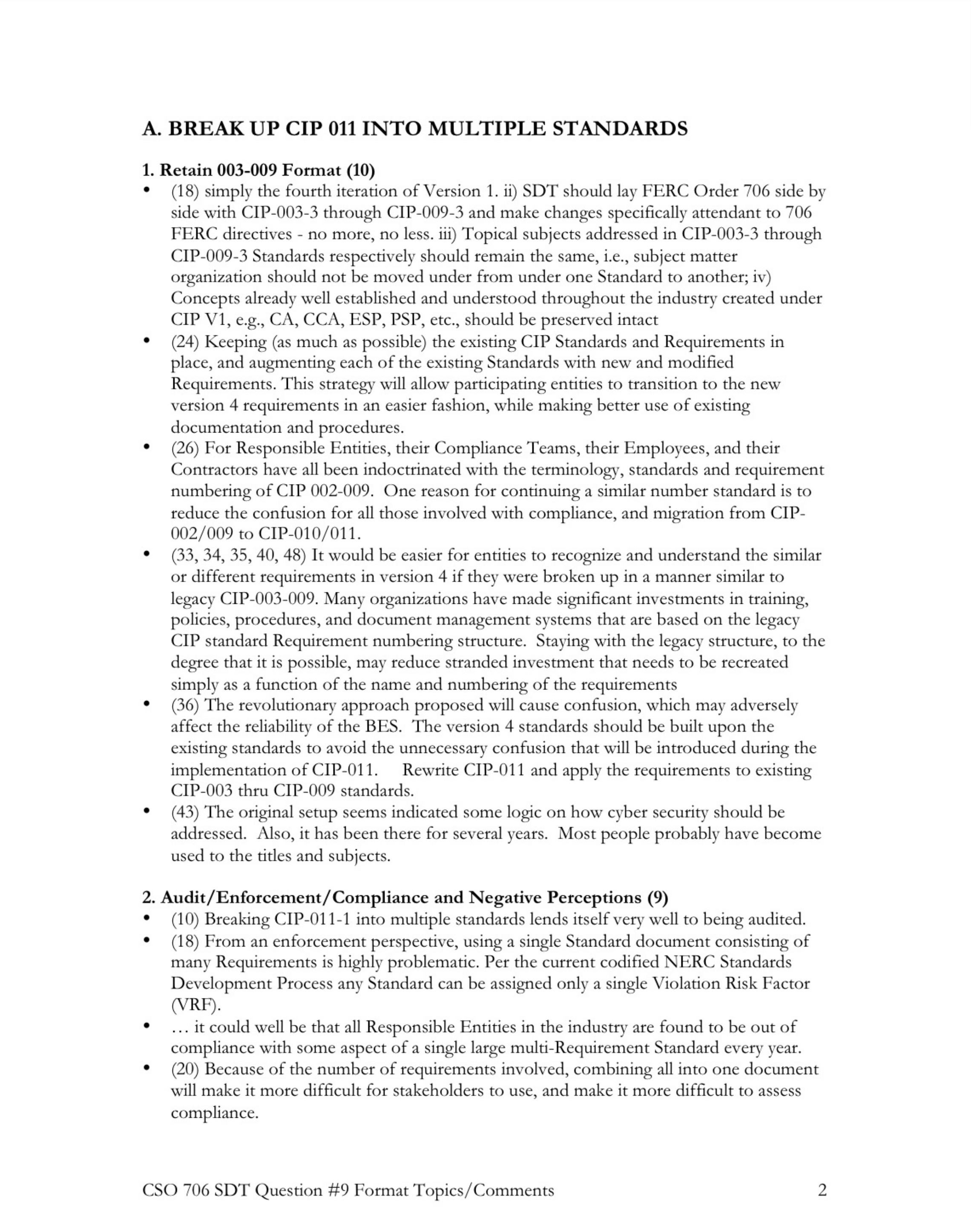
1. Retain 003-009 Format *(10 comments)*
2. Audit/Enforcement/Compliance and Negative Perceptions *(9 comments)*
3. Suggested Standard Format Combinations *(8 comments)*
4. Level of Effort and Cost of Changing Format *(6 comments)*
5. Use Functional Areas *(3 comments)*
6. Consistency with Other Industry Cyber Protection Standards *(2 comments)*
7. Makes Easier Ownership Assignment and Referencing *(1 comment)*
8. Monitoring Changes *(1 comment)*
9. Aids the Revision Process *(1 comment)*
10. Focus on Security *(1 comment)*
11. Approve as a Complete Set *(1 comment)*
12. CIP Standards Should Stand Alone *(1 comment)*

KEEP AS A SINGLE 011

1. Better Organization and Organizational Review *(8 comments)*
2. Auditing and Multiple Violations of Single Standard. *(6 comments)*
3. Format *(2 comments)*
4. Table Format *(1 comment)*
5. Revisions *(1comment)*
6. Alignment with Other Standards *(1comment)*

C. NO PREFERENCE

1. Implementation, Updates and Revisions *(4 comments)*
2. Focus on Defining Auditable Requirements. *(3 comments)*
3. Reporting at a Requirement Level *(2comments)*
4. Simpler Management *(2 comments)*
5. Table Format *(1comment)*



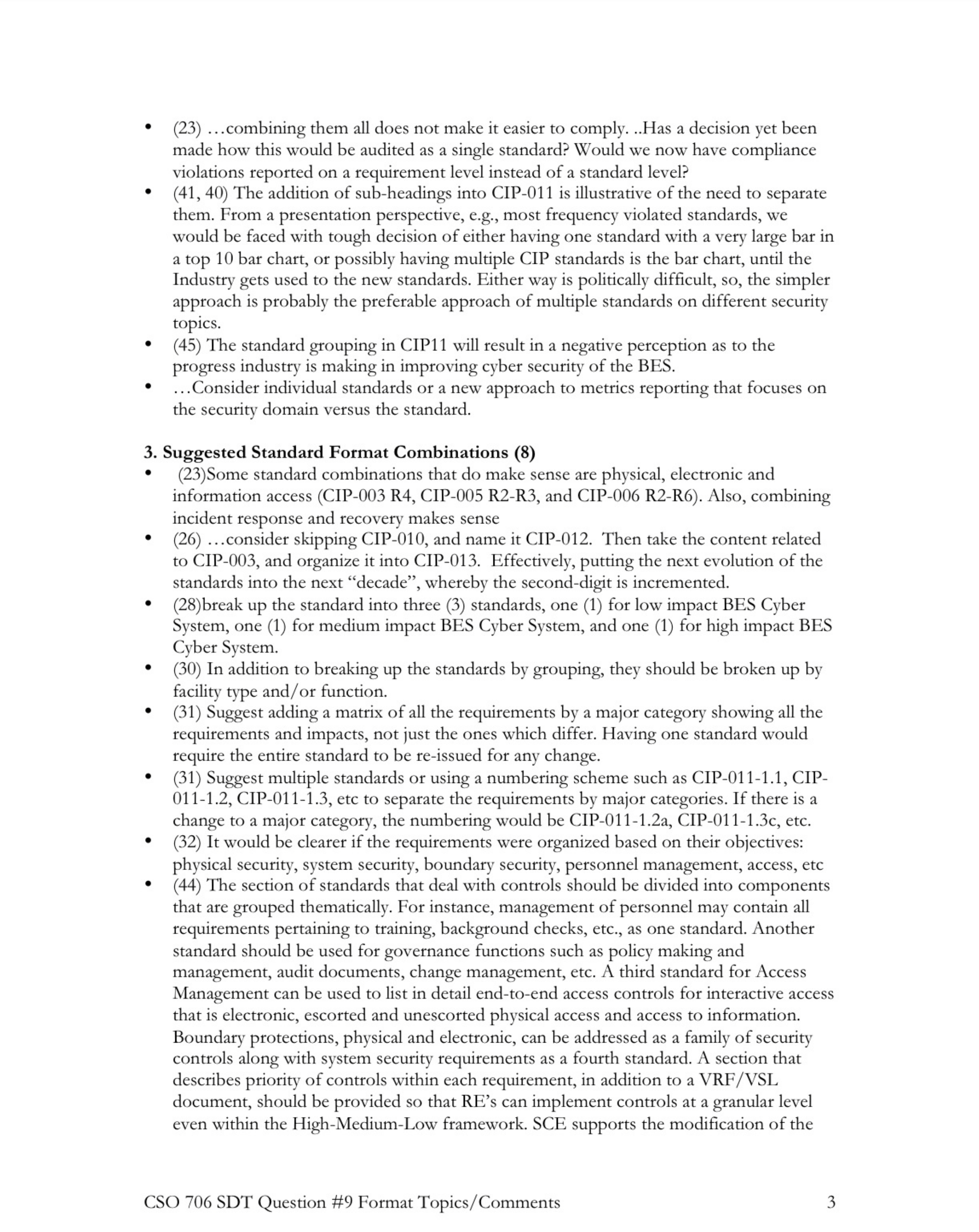
A. BREAK UP CIP 011 INTO MULTIPLE STANDARDS

1. Retain 003-009 Format (10)

- (18) simply the fourth iteration of Version 1. ii) SDT should lay FERC Order 706 side by side with CIP-003-3 through CIP-009-3 and make changes specifically attendant to 706 FERC directives - no more, no less. iii) Topical subjects addressed in CIP-003-3 through CIP-009-3 Standards respectively should remain the same, i.e., subject matter organization should not be moved under from under one Standard to another; iv) Concepts already well established and understood throughout the industry created under CIP V1, e.g., CA, CCA, ESP, PSP, etc., should be preserved intact
- (24) Keeping (as much as possible) the existing CIP Standards and Requirements in place, and augmenting each of the existing Standards with new and modified Requirements. This strategy will allow participating entities to transition to the new version 4 requirements in an easier fashion, while making better use of existing documentation and procedures.
- (26) For Responsible Entities, their Compliance Teams, their Employees, and their Contractors have all been indoctrinated with the terminology, standards and requirement numbering of CIP 002-009. One reason for continuing a similar number standard is to reduce the confusion for all those involved with compliance, and migration from CIP-002/009 to CIP-010/011.
- (33, 34, 35, 40, 48) It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements
- (36) The revolutionary approach proposed will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
- (43) The original setup seems indicated some logic on how cyber security should be addressed. Also, it has been there for several years. Most people probably have become used to the titles and subjects.

2. Audit/Enforcement/Compliance and Negative Perceptions (9)

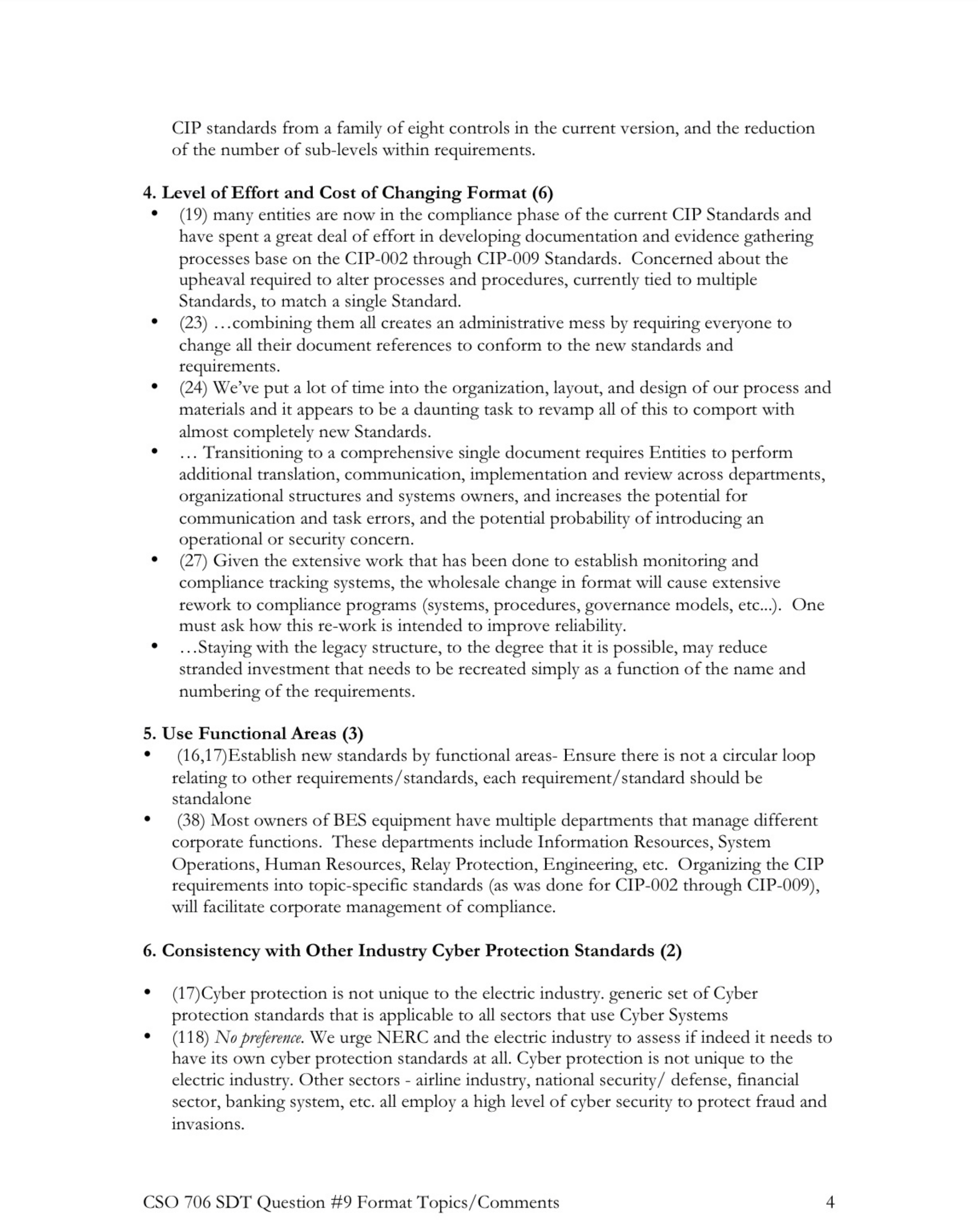
- (10) Breaking CIP-011-1 into multiple standards lends itself very well to being audited.
- (18) From an enforcement perspective, using a single Standard document consisting of many Requirements is highly problematic. Per the current codified NERC Standards Development Process any Standard can be assigned only a single Violation Risk Factor (VRF).
- … it could well be that all Responsible Entities in the industry are found to be out of compliance with some aspect of a single large multi-Requirement Standard every year.
- (20) Because of the number of requirements involved, combining all into one document will make it more difficult for stakeholders to use, and make it more difficult to assess compliance.



- (23) …combining them all does not make it easier to comply. ..Has a decision yet been made how this would be audited as a single standard? Would we now have compliance violations reported on a requirement level instead of a standard level?
- (41, 40) The addition of sub-headings into CIP-011 is illustrative of the need to separate them. From a presentation perspective, e.g., most frequency violated standards, we would be faced with tough decision of either having one standard with a very large bar in a top 10 bar chart, or possibly having multiple CIP standards is the bar chart, until the Industry gets used to the new standards. Either way is politically difficult, so, the simpler approach is probably the preferable approach of multiple standards on different security topics.
- (45) The standard grouping in CIP11 will result in a negative perception as to the progress industry is making in improving cyber security of the BES.
- …Consider individual standards or a new approach to metrics reporting that focuses on the security domain versus the standard.

3. Suggested Standard Format Combinations (8)

- (23)Some standard combinations that do make sense are physical, electronic and information access (CIP-003 R4, CIP-005 R2-R3, and CIP-006 R2-R6). Also, combining incident response and recovery makes sense
- (26) …consider skipping CIP-010, and name it CIP-012. Then take the content related to CIP-003, and organize it into CIP-013. Effectively, putting the next evolution of the standards into the next "decade", whereby the second-digit is incremented.
- (28)break up the standard into three (3) standards, one (1) for low impact BES Cyber System, one (1) for medium impact BES Cyber System, and one (1) for high impact BES Cyber System.
- (30) In addition to breaking up the standards by grouping, they should be broken up by facility type and/or function.
- (31) Suggest adding a matrix of all the requirements by a major category showing all the requirements and impacts, not just the ones which differ. Having one standard would require the entire standard to be re-issued for any change.
- (31) Suggest multiple standards or using a numbering scheme such as CIP-011-1.1, CIP-011-1.2, CIP-011-1.3, etc to separate the requirements by major categories. If there is a change to a major category, the numbering would be CIP-011-1.2a, CIP-011-1.3c, etc.
- (32) It would be clearer if the requirements were organized based on their objectives: physical security, system security, boundary security, personnel management, access, etc
- (44) The section of standards that deal with controls should be divided into components that are grouped thematically. For instance, management of personnel may contain all requirements pertaining to training, background checks, etc., as one standard. Another standard should be used for governance functions such as policy making and management, audit documents, change management, etc. A third standard for Access Management can be used to list in detail end-to-end access controls for interactive access that is electronic, escorted and unescorted physical access and access to information. Boundary protections, physical and electronic, can be addressed as a family of security controls along with system security requirements as a fourth standard. A section that describes priority of controls within each requirement, in addition to a VRF/VSL document, should be provided so that RE's can implement controls at a granular level even within the High-Medium-Low framework. SCE supports the modification of the



CIP standards from a family of eight controls in the current version, and the reduction of the number of sub-levels within requirements.

4. Level of Effort and Cost of Changing Format (6)

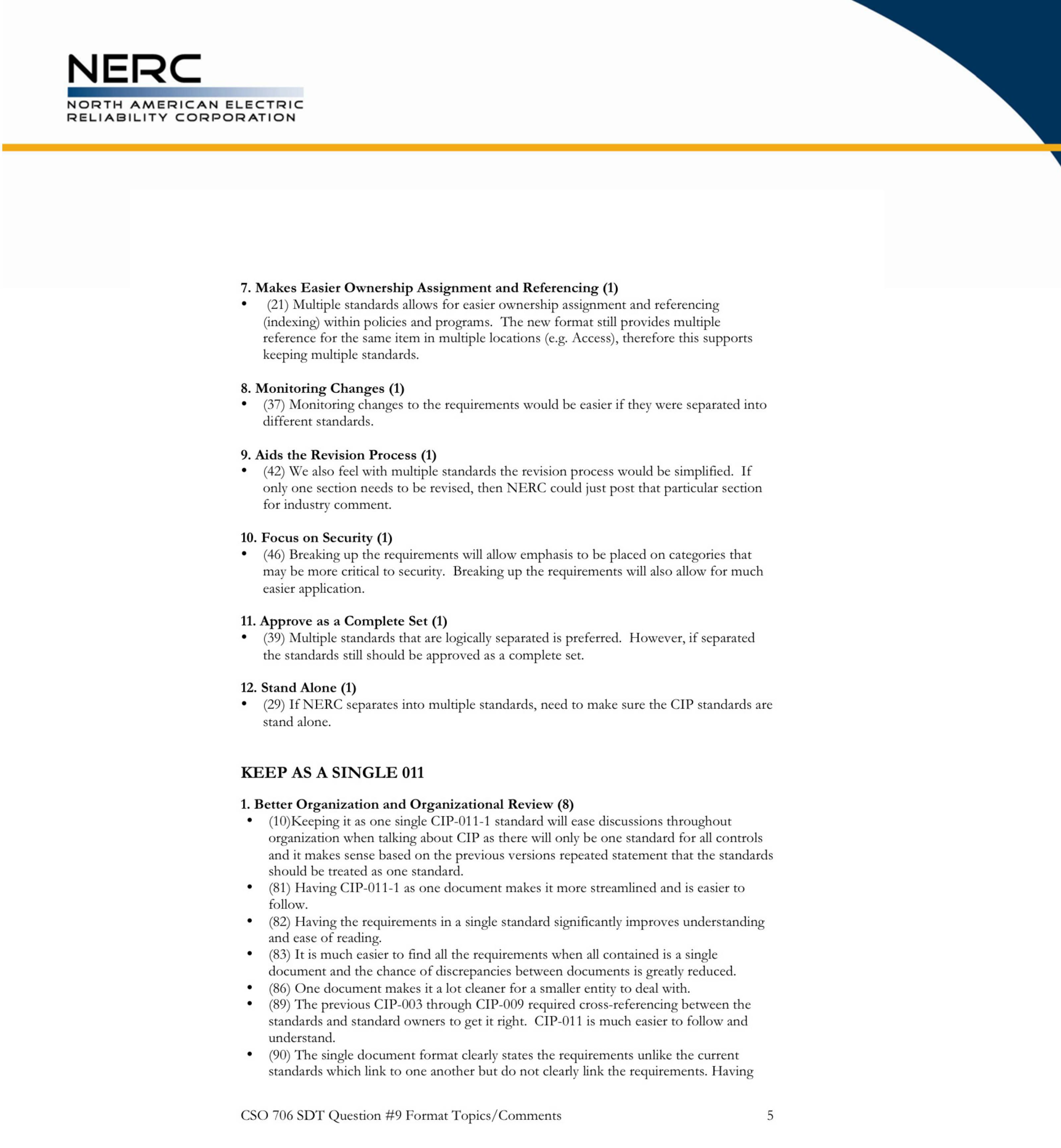
- (19) many entities are now in the compliance phase of the current CIP Standards and have spent a great deal of effort in developing documentation and evidence gathering processes base on the CIP-002 through CIP-009 Standards. Concerned about the upheaval required to alter processes and procedures, currently tied to multiple Standards, to match a single Standard.
- (23) …combining them all creates an administrative mess by requiring everyone to change all their document references to conform to the new standards and requirements.
- (24) We've put a lot of time into the organization, layout, and design of our process and materials and it appears to be a daunting task to revamp all of this to comport with almost completely new Standards.
- … Transitioning to a comprehensive single document requires Entities to perform additional translation, communication, implementation and review across departments, organizational structures and systems owners, and increases the potential for communication and task errors, and the potential probability of introducing an operational or security concern.
- (27) Given the extensive work that has been done to establish monitoring and compliance tracking systems, the wholesale change in format will cause extensive rework to compliance programs (systems, procedures, governance models, etc...). One must ask how this re-work is intended to improve reliability.
- …Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

5. Use Functional Areas (3)

- (16,17)Establish new standards by functional areas- Ensure there is not a circular loop relating to other requirements/standards, each requirement/standard should be standalone
- (38) Most owners of BES equipment have multiple departments that manage different corporate functions. These departments include Information Resources, System Operations, Human Resources, Relay Protection, Engineering, etc. Organizing the CIP requirements into topic-specific standards (as was done for CIP-002 through CIP-009), will facilitate corporate management of compliance.

6. Consistency with Other Industry Cyber Protection Standards (2)

- (17)Cyber protection is not unique to the electric industry. generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems
- (118) *No preference.* We urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions.



NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

7. Makes Easier Ownership Assignment and Referencing (1)

- (21) Multiple standards allows for easier ownership assignment and referencing (indexing) within policies and programs. The new format still provides multiple reference for the same item in multiple locations (e.g. Access), therefore this supports keeping multiple standards.

8. Monitoring Changes (1)

- (37) Monitoring changes to the requirements would be easier if they were separated into different standards.

9. Aids the Revision Process (1)

- (42) We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.

10. Focus on Security (1)

- (46) Breaking up the requirements will allow emphasis to be placed on categories that may be more critical to security. Breaking up the requirements will also allow for much easier application.

11. Approve as a Complete Set (1)

- (39) Multiple standards that are logically separated is preferred. However, if separated the standards still should be approved as a complete set.

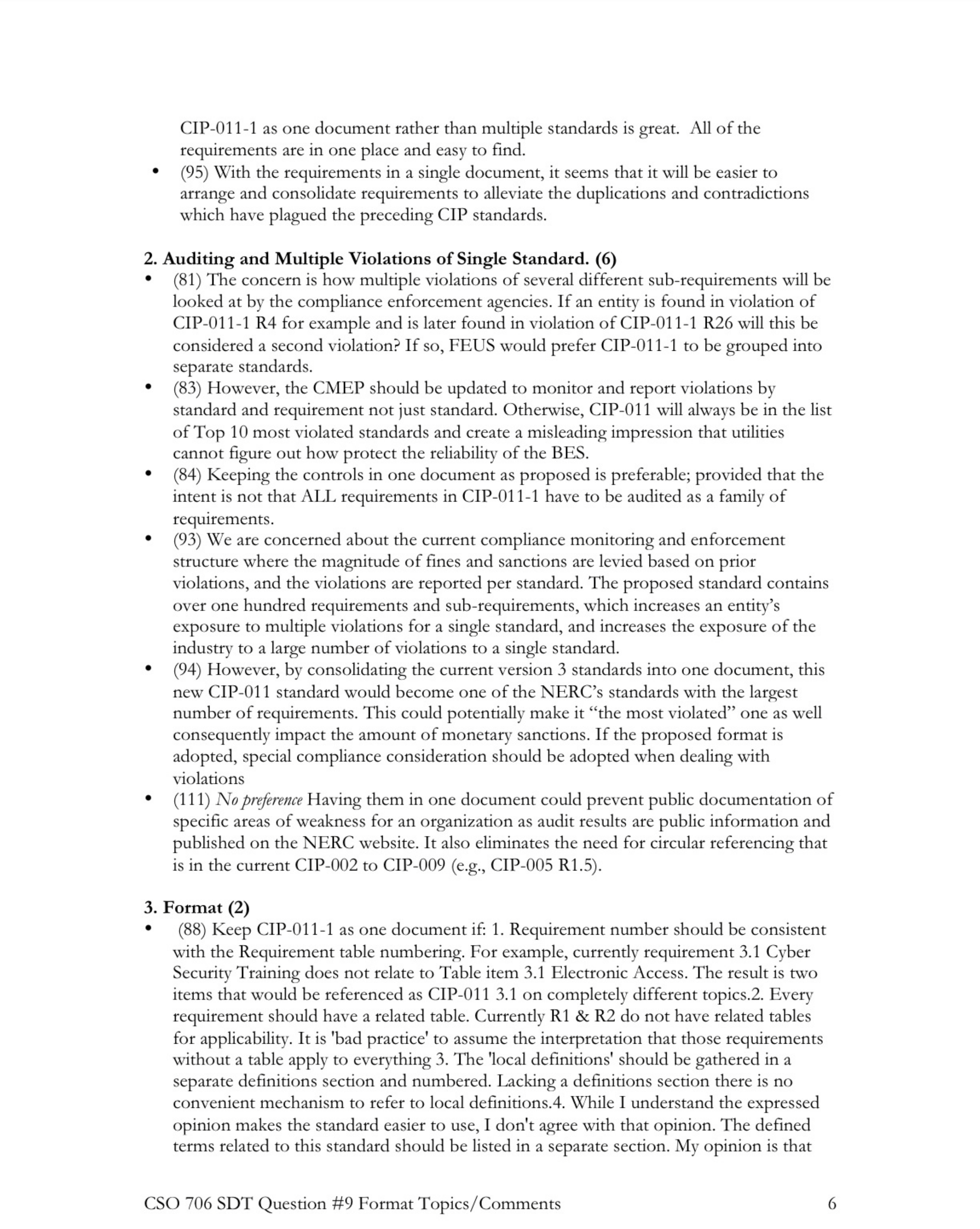
12. Stand Alone (1)

- (29) If NERC separates into multiple standards, need to make sure the CIP standards are stand alone.

KEEP AS A SINGLE 011

1. Better Organization and Organizational Review (8)

- (10)Keeping it as one single CIP-011-1 standard will ease discussions throughout organization when talking about CIP as there will only be one standard for all controls and it makes sense based on the previous versions repeated statement that the standards should be treated as one standard.
- (81) Having CIP-011-1 as one document makes it more streamlined and is easier to follow.
- (82) Having the requirements in a single standard significantly improves understanding and ease of reading.
- (83) It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced.
- (86) One document makes it a lot cleaner for a smaller entity to deal with.
- (89) The previous CIP-003 through CIP-009 required cross-referencing between the standards and standard owners to get it right. CIP-011 is much easier to follow and understand.
- (90) The single document format clearly states the requirements unlike the current standards which link to one another but do not clearly link the requirements. Having



CIP-011-1 as one document rather than multiple standards is great. All of the requirements are in one place and easy to find.

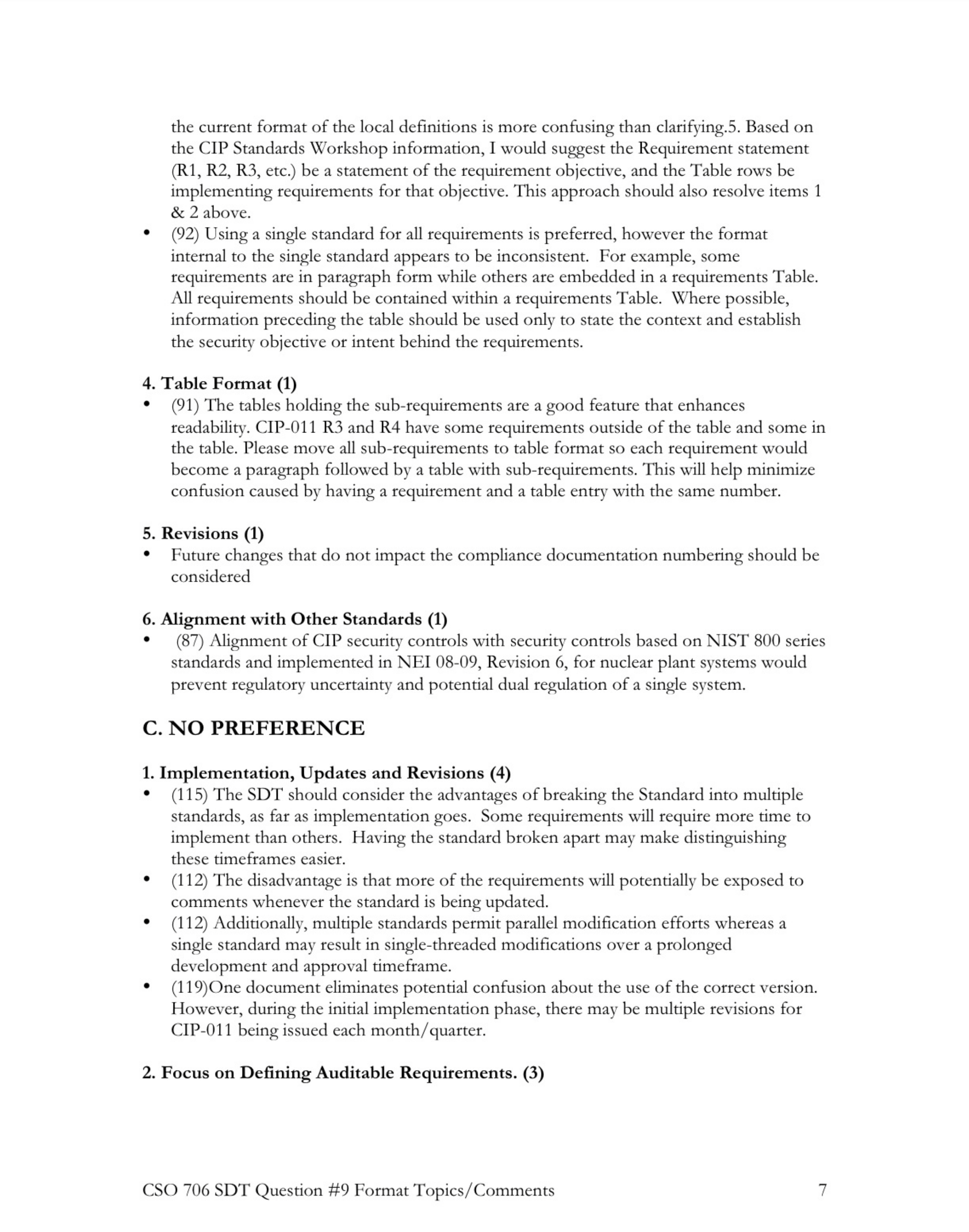
- (95) With the requirements in a single document, it seems that it will be easier to arrange and consolidate requirements to alleviate the duplications and contradictions which have plagued the preceding CIP standards.

2. Auditing and Multiple Violations of Single Standard. (6)

- (81) The concern is how multiple violations of several different sub-requirements will be looked at by the compliance enforcement agencies. If an entity is found in violation of CIP-011-1 R4 for example and is later found in violation of CIP-011-1 R26 will this be considered a second violation? If so, FEUS would prefer CIP-011-1 to be grouped into separate standards.
- (83) However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
- (84) Keeping the controls in one document as proposed is preferable; provided that the intent is not that ALL requirements in CIP-011-1 have to be audited as a family of requirements.
- (93) We are concerned about the current compliance monitoring and enforcement structure where the magnitude of fines and sanctions are levied based on prior violations, and the violations are reported per standard. The proposed standard contains over one hundred requirements and sub-requirements, which increases an entity's exposure to multiple violations for a single standard, and increases the exposure of the industry to a large number of violations to a single standard.
- (94) However, by consolidating the current version 3 standards into one document, this new CIP-011 standard would become one of the NERC's standards with the largest number of requirements. This could potentially make it "the most violated" one as well consequently impact the amount of monetary sanctions. If the proposed format is adopted, special compliance consideration should be adopted when dealing with violations
- (111) *No preference* Having them in one document could prevent public documentation of specific areas of weakness for an organization as audit results are public information and published on the NERC website. It also eliminates the need for circular referencing that is in the current CIP-002 to CIP-009 (e.g., CIP-005 R1.5).

3. Format (2)

- (88) Keep CIP-011-1 as one document if: 1. Requirement number should be consistent with the Requirement table numbering. For example, currently requirement 3.1 Cyber Security Training does not relate to Table item 3.1 Electronic Access. The result is two items that would be referenced as CIP-011 3.1 on completely different topics.2. Every requirement should have a related table. Currently R1 & R2 do not have related tables for applicability. It is 'bad practice' to assume the interpretation that those requirements without a table apply to everything 3. The 'local definitions' should be gathered in a separate definitions section and numbered. Lacking a definitions section there is no convenient mechanism to refer to local definitions.4. While I understand the expressed opinion makes the standard easier to use, I don't agree with that opinion. The defined terms related to this standard should be listed in a separate section. My opinion is that



the current format of the local definitions is more confusing than clarifying.5. Based on the CIP Standards Workshop information, I would suggest the Requirement statement (R1, R2, R3, etc.) be a statement of the requirement objective, and the Table rows be implementing requirements for that objective. This approach should also resolve items 1 & 2 above.

- (92) Using a single standard for all requirements is preferred, however the format internal to the single standard appears to be inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.

4. Table Format (1)

- (91) The tables holding the sub-requirements are a good feature that enhances readability. CIP-011 R3 and R4 have some requirements outside of the table and some in the table. Please move all sub-requirements to table format so each requirement would become a paragraph followed by a table with sub-requirements. This will help minimize confusion caused by having a requirement and a table entry with the same number.

5. Revisions (1)

- Future changes that do not impact the compliance documentation numbering should be considered

6. Alignment with Other Standards (1)

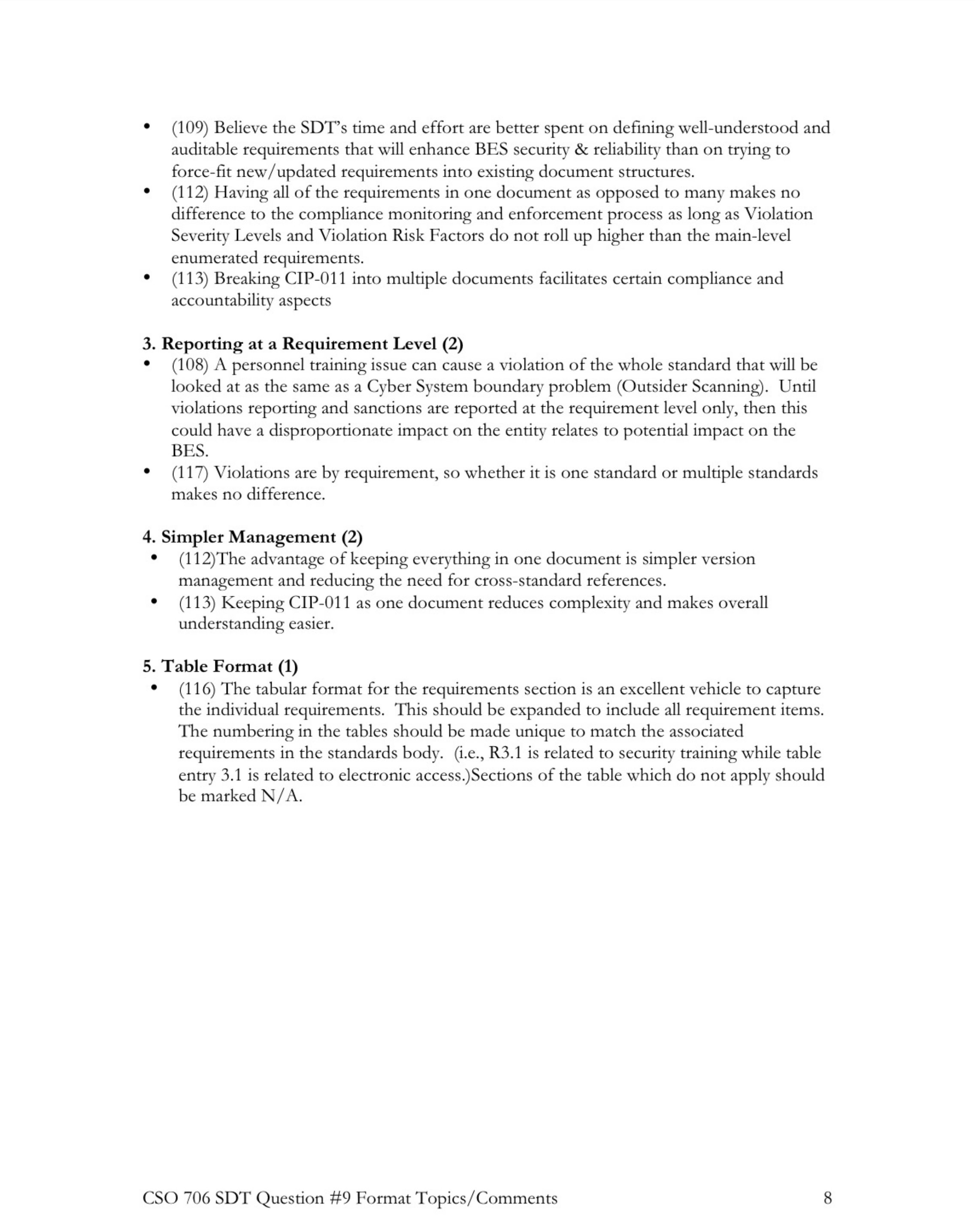
- (87) Alignment of CIP security controls with security controls based on NIST 800 series standards and implemented in NEI 08-09, Revision 6, for nuclear plant systems would prevent regulatory uncertainty and potential dual regulation of a single system.

C. NO PREFERENCE

1. Implementation, Updates and Revisions (4)

- (115) The SDT should consider the advantages of breaking the Standard into multiple standards, as far as implementation goes. Some requirements will require more time to implement than others. Having the standard broken apart may make distinguishing these timeframes easier.
- (112) The disadvantage is that more of the requirements will potentially be exposed to comments whenever the standard is being updated.
- (112) Additionally, multiple standards permit parallel modification efforts whereas a single standard may result in single-threaded modifications over a prolonged development and approval timeframe.
- (119)One document eliminates potential confusion about the use of the correct version. However, during the initial implementation phase, there may be multiple revisions for CIP-011 being issued each month/quarter.

2. Focus on Defining Auditable Requirements. (3)



- (109) Believe the SDT's time and effort are better spent on defining well-understood and auditable requirements that will enhance BES security & reliability than on trying to force-fit new/updated requirements into existing document structures.
- (112) Having all of the requirements in one document as opposed to many makes no difference to the compliance monitoring and enforcement process as long as Violation Severity Levels and Violation Risk Factors do not roll up higher than the main-level enumerated requirements.
- (113) Breaking CIP-011 into multiple documents facilitates certain compliance and accountability aspects

3. Reporting at a Requirement Level (2)

- (108) A personnel training issue can cause a violation of the whole standard that will be looked at as the same as a Cyber System boundary problem (Outsider Scanning). Until violations reporting and sanctions are reported at the requirement level only, then this could have a disproportionate impact on the entity relates to potential impact on the BES.
- (117) Violations are by requirement, so whether it is one standard or multiple standards makes no difference.

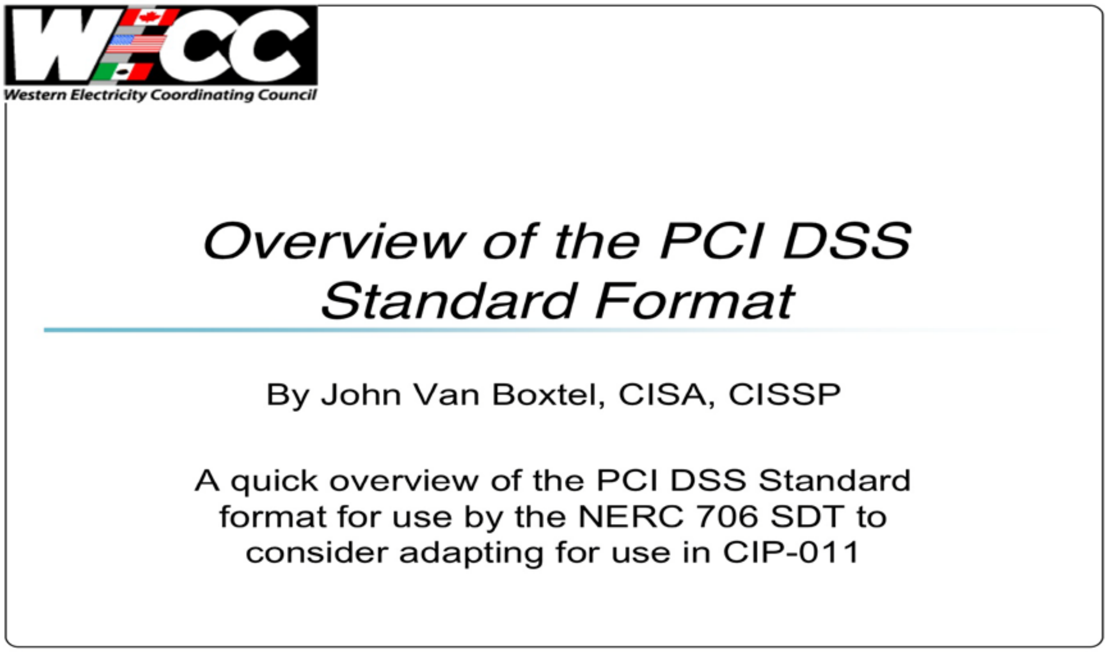
4. Simpler Management (2)

- (112)The advantage of keeping everything in one document is simpler version management and reducing the need for cross-standard references.
- (113) Keeping CIP-011 as one document reduces complexity and makes overall understanding easier.

5. Table Format (1)

- (116) The tabular format for the requirements section is an excellent vehicle to capture the individual requirements. This should be expanded to include all requirement items. The numbering in the tables should be made unique to match the associated requirements in the standards body. (i.e., R3.1 is related to security training while table entry 3.1 is related to electronic access.)Sections of the table which do not apply should be marked N/A.

Appendix # 9 Format Consideration- John Van Boxtel Presentation

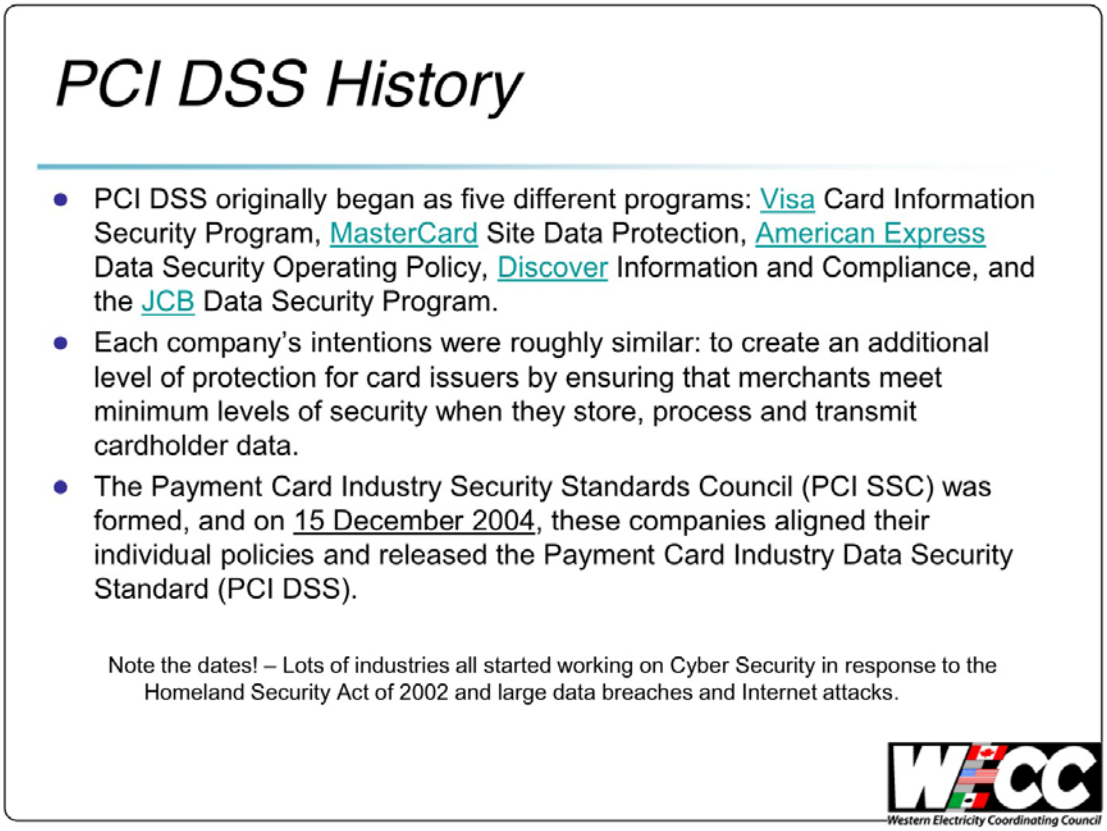


Western Electricity Coordinating Council

Overview of the PCI DSS Standard Format

By John Van Boxtel, CISA, CISSP

A quick overview of the PCI DSS Standard format for use by the NERC 706 SDT to consider adapting for use in CIP-011

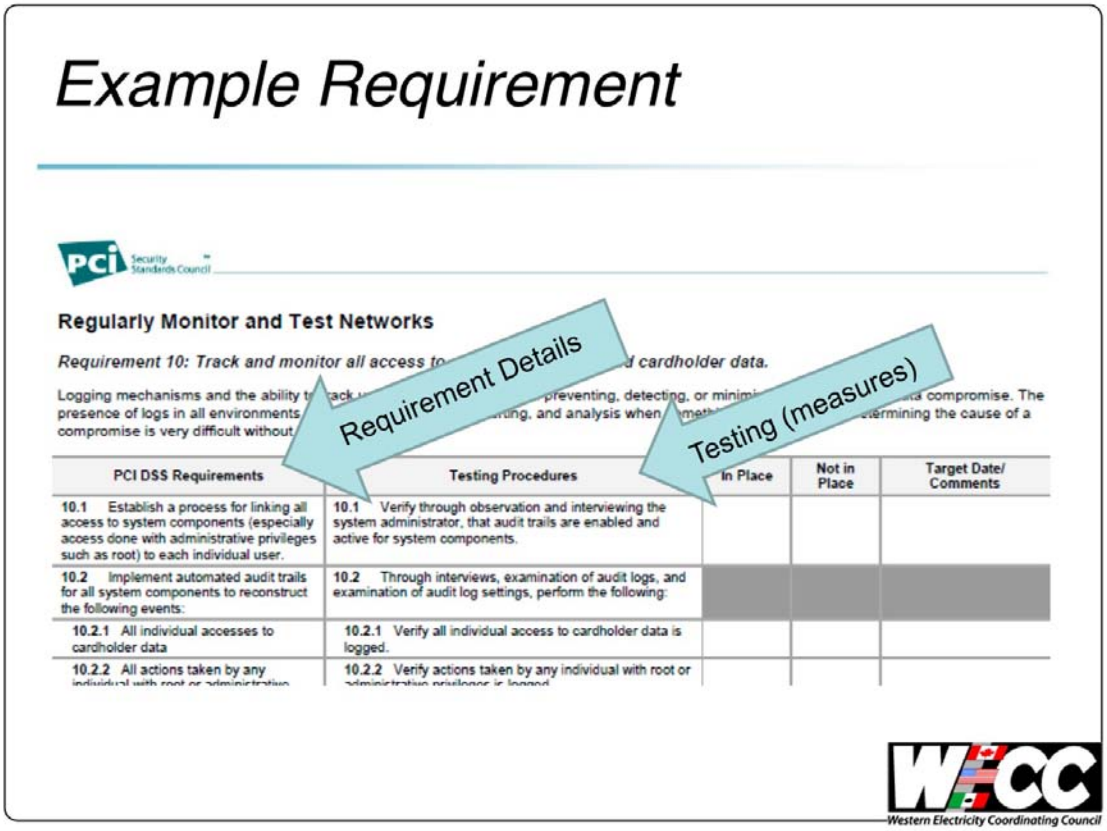


PCI DSS History

- PCI DSS originally began as five different programs: Visa Card Information Security Program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and the JCB Data Security Program.
- Each company's intentions were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data.
- The Payment Card Industry Security Standards Council (PCI SSC) was formed, and on 15 December 2004, these companies aligned their individual policies and released the Payment Card Industry Data Security Standard (PCI DSS).

Note the dates! – Lots of industries all started working on Cyber Security in response to the Homeland Security Act of 2002 and large data breaches and Internet attacks.

Western Electricity Coordinating Council



Example Requirement

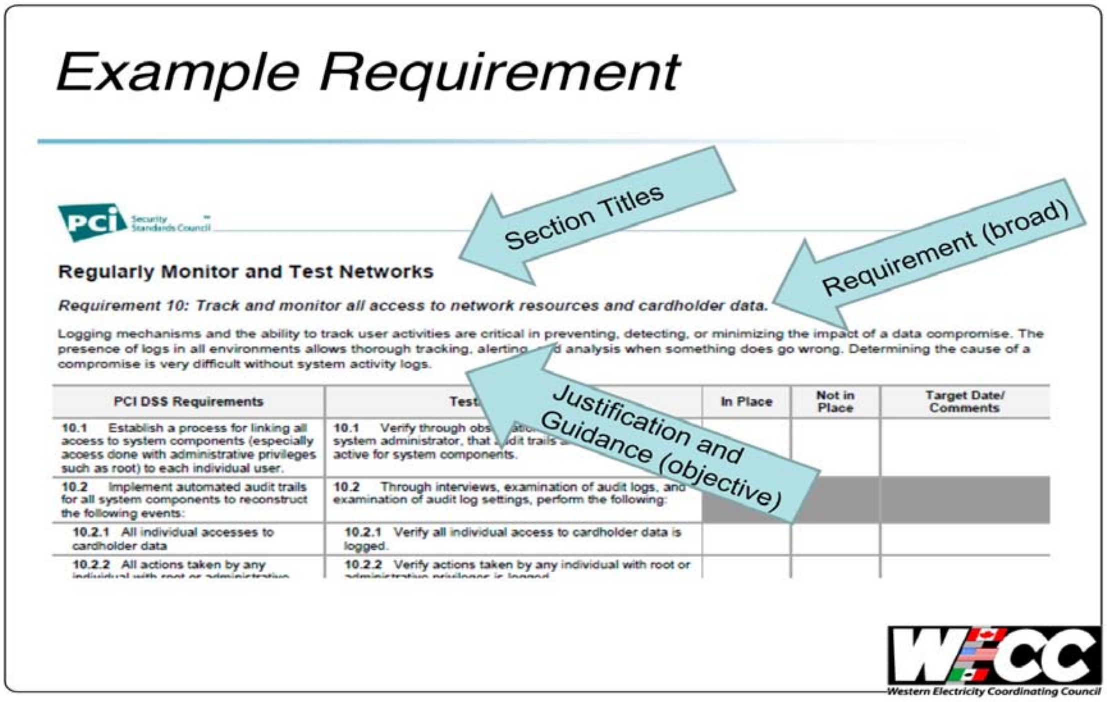
PCI Security Standards Council
Requirement Details
Testing (measures)
WECC
Western Electricity Coordinating Council

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to ***d cardholder data.***

Logging mechanisms and the ability t rack preventing, detecting, or minimi compromise. The presence of logs in all environments ting, and analysis when meth termining the cause of a compromise is very difficult without

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any individual with root or administrative	**10.2.2** Verify actions taken by any individual with root or administrative privileges is logged.			



Example Requirement

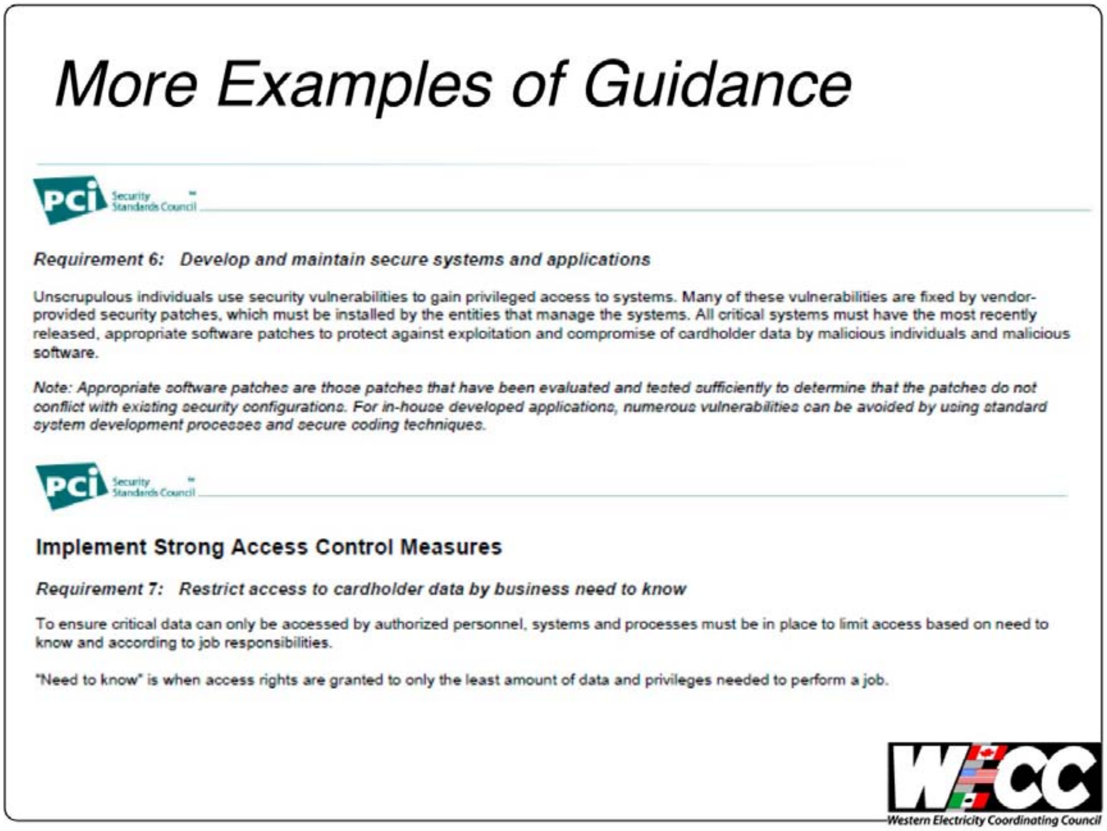
PCI Security Standards Council
Section Titles
Requirement (broad)
Justification and Guidance (objective)
WECC
Western Electricity Coordinating Council

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS Requirements	Testi	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through obs system administrator, that dit trails active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any individual with root or administrative	**10.2.2** Verify actions taken by any individual with root or administrative privileges is logged.			



More Examples of Guidance

PCI Security Standards Council™

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI Security Standards Council™

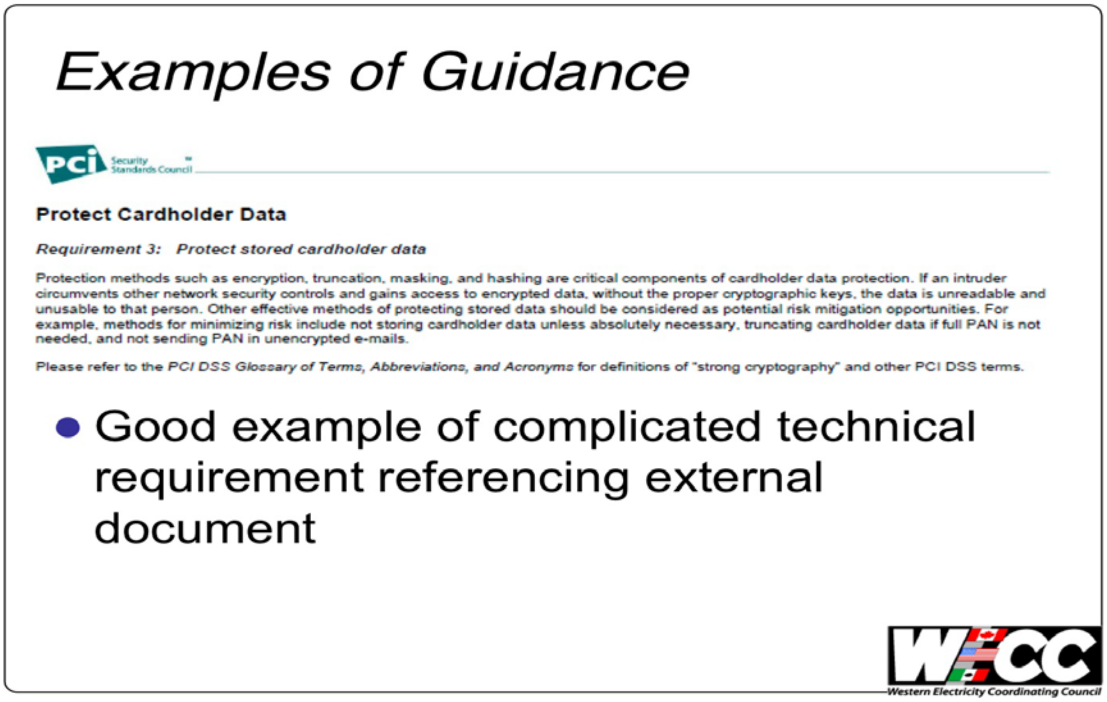
Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

WECC
Western Electricity Coordinating Council



Examples of Guidance

PCI Security Standards Council™

Protect Cardholder Data

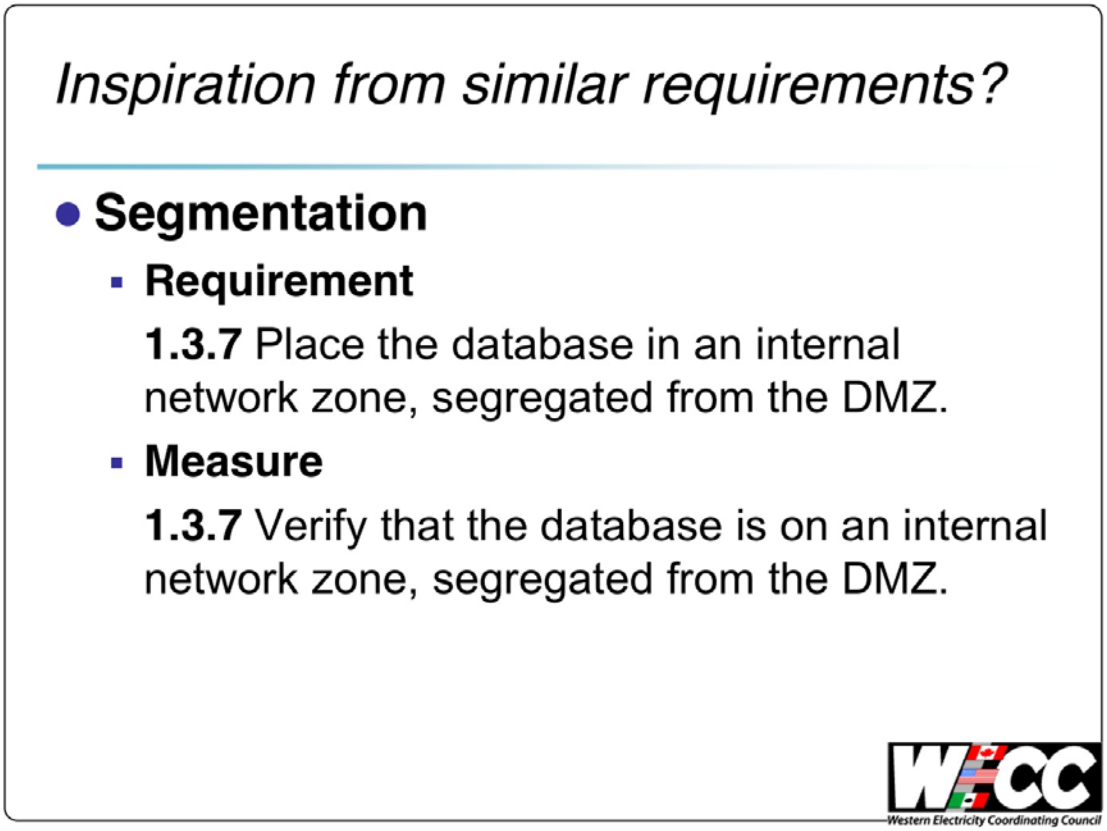
Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

Please refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

- Good example of complicated technical requirement referencing external document

WECC
Western Electricity Coordinating Council



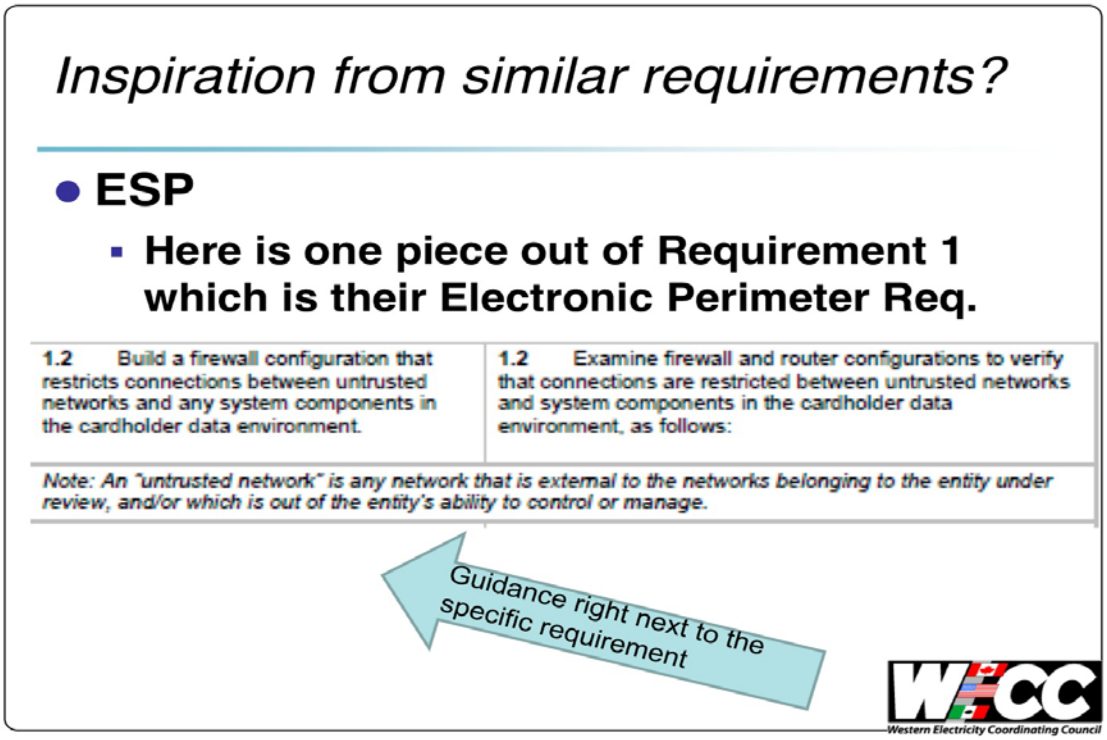
Inspiration from similar requirements?

- **Segmentation**
  - **Requirement**

    1.3.7 Place the database in an internal network zone, segregated from the DMZ.
  - **Measure**

    1.3.7 Verify that the database is on an internal network zone, segregated from the DMZ.

Western Electricity Coordinating Council



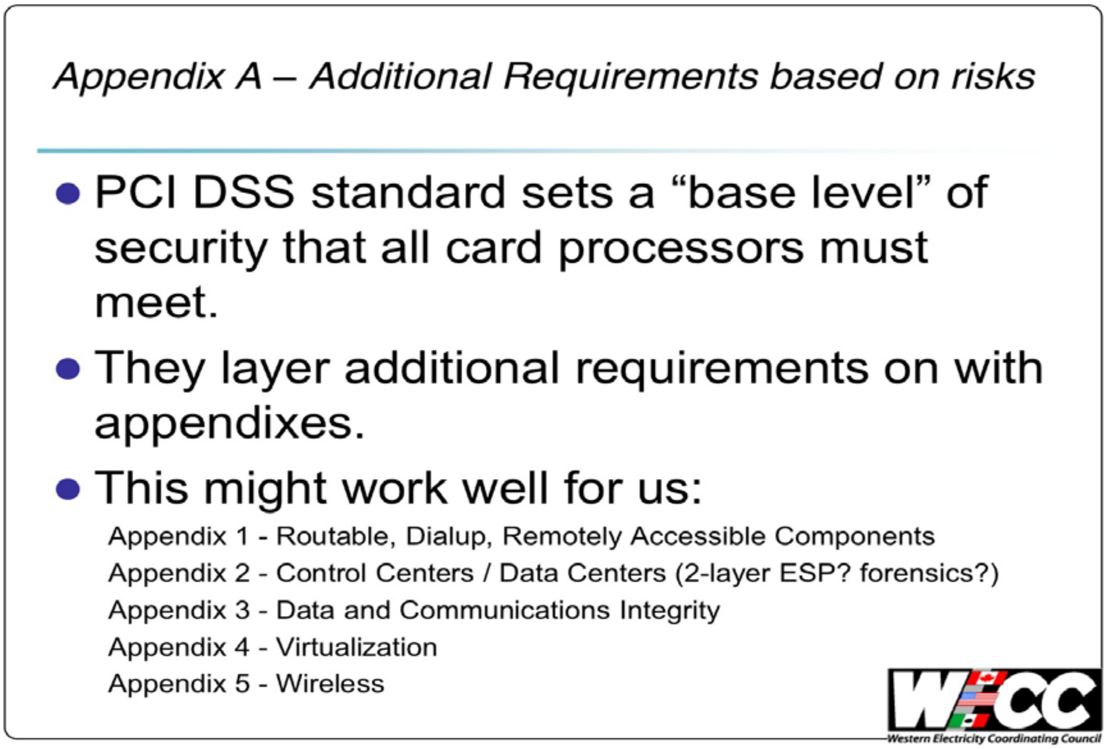
Inspiration from similar requirements?

- **ESP**
  - **Here is one piece out of Requirement 1 which is their Electronic Perimeter Req.**

1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:
Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	

Guidance right next to the specific requirement

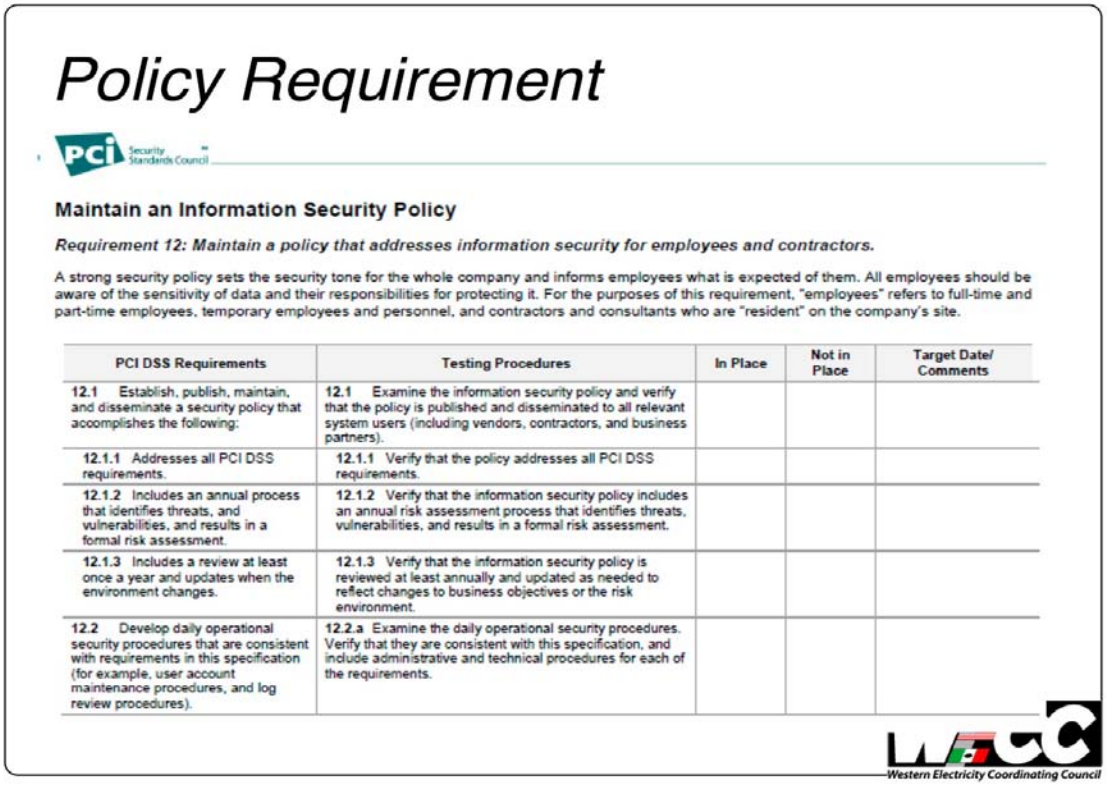
Western Electricity Coordinating Council



Appendix A – Additional Requirements based on risks

- PCI DSS standard sets a “base level” of security that all card processors must meet.
- They layer additional requirements on with appendixes.
- This might work well for us:

  Appendix 1 - Routable, Dialup, Remotely Accessible Components
  Appendix 2 - Control Centers / Data Centers (2-layer ESP? forensics?)
  Appendix 3 - Data and Communications Integrity
  Appendix 4 - Virtualization
  Appendix 5 - Wireless



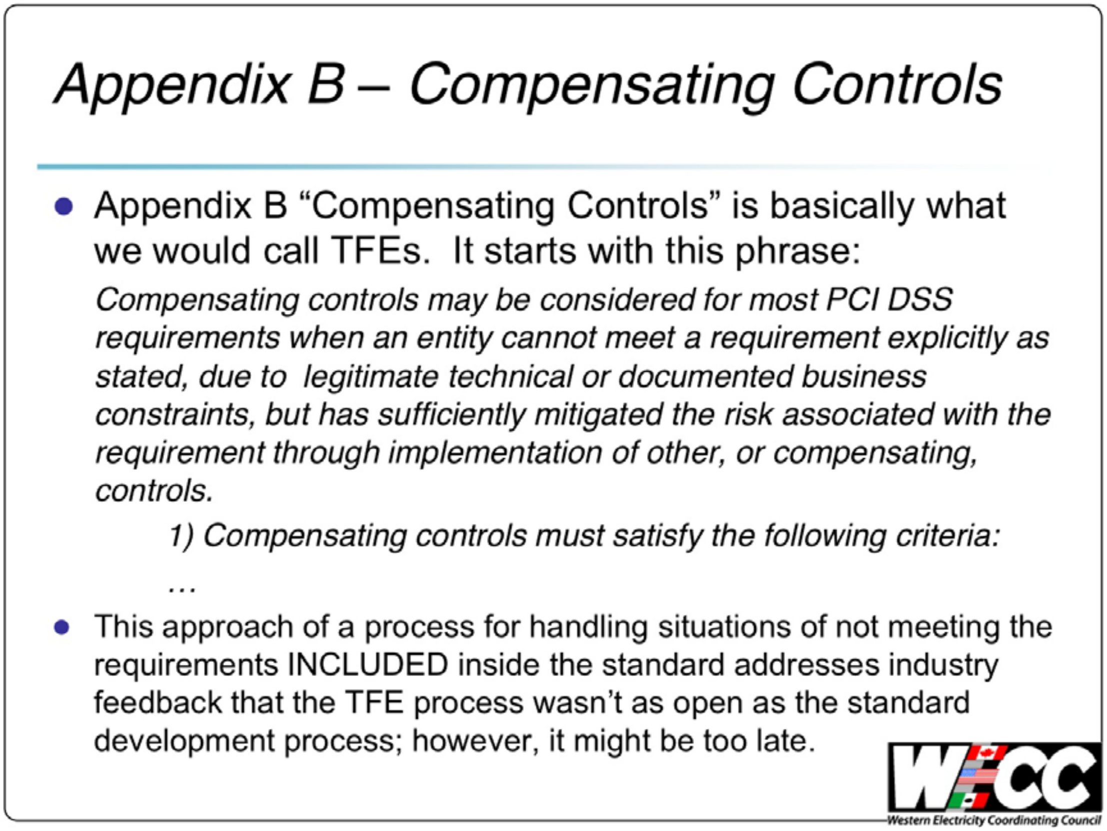
Policy Requirement

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners).			
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.			
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	**12.1.2** Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.			
12.1.3 Includes a review at least once a year and updates when the environment changes.	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.			
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2.a** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.			



Appendix B – Compensating Controls

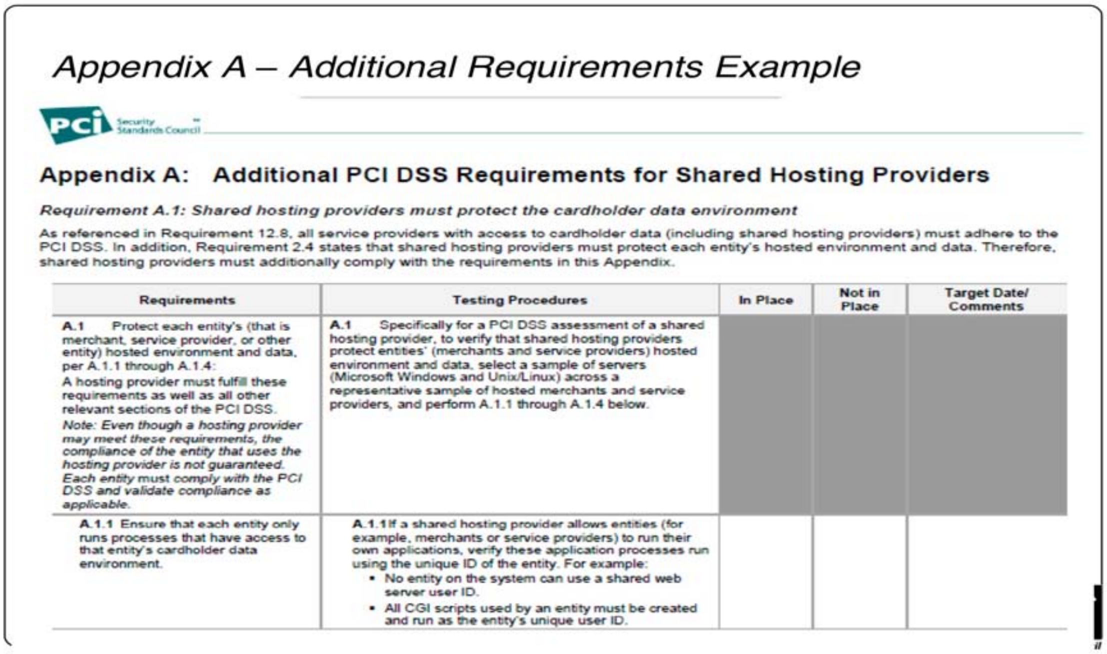
- Appendix B “Compensating Controls” is basically what we would call TFEs. It starts with this phrase:

  Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

  1) Compensating controls must satisfy the following criteria:

  …
- This approach of a process for handling situations of not meeting the requirements INCLUDED inside the standard addresses industry feedback that the TFE process wasn’t as open as the standard development process; however, it might be too late.

Western Electricity Coordinating Council



Appendix A – Additional Requirements Example

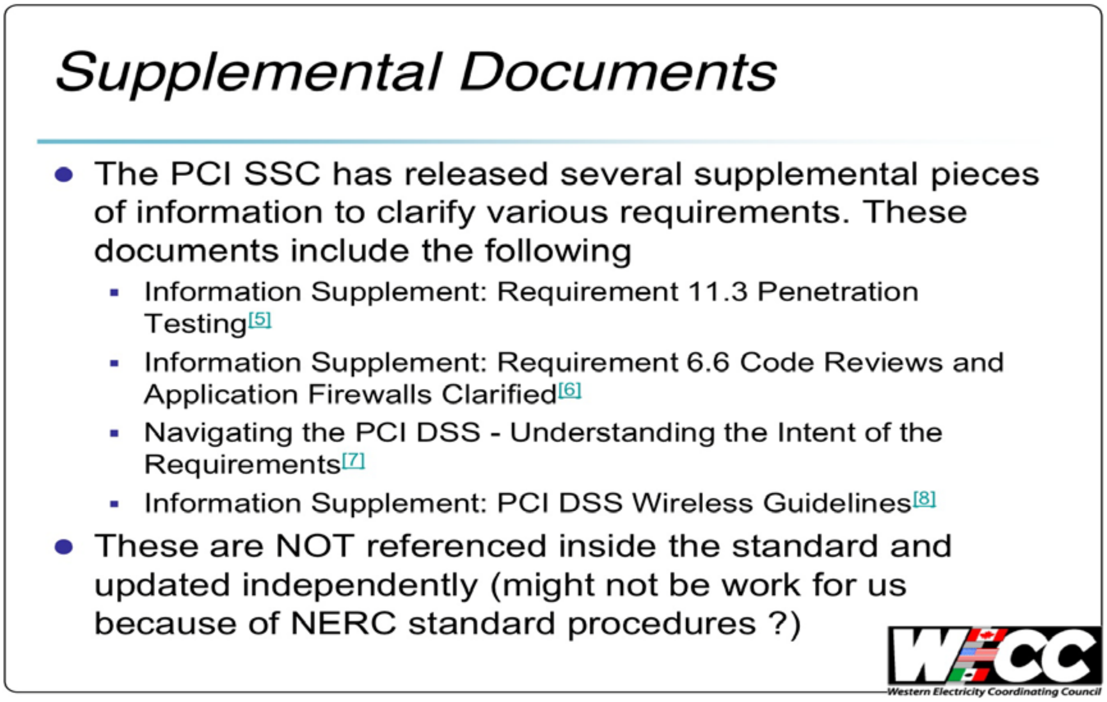
PCI Security Standards Council

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect the cardholder data environment

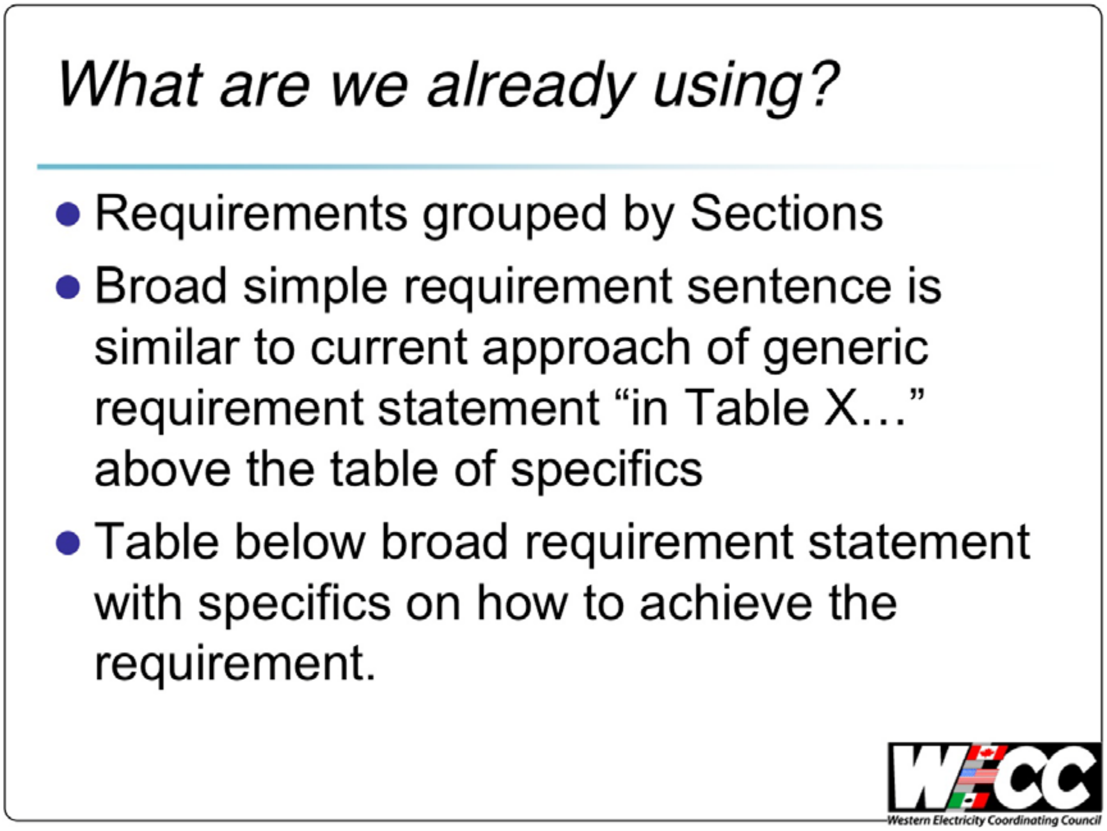
As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below.			
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: ▪ No entity on the system can use a shared web server user ID. ▪ All CGI scripts used by an entity must be created and run as the entity's unique user ID.			



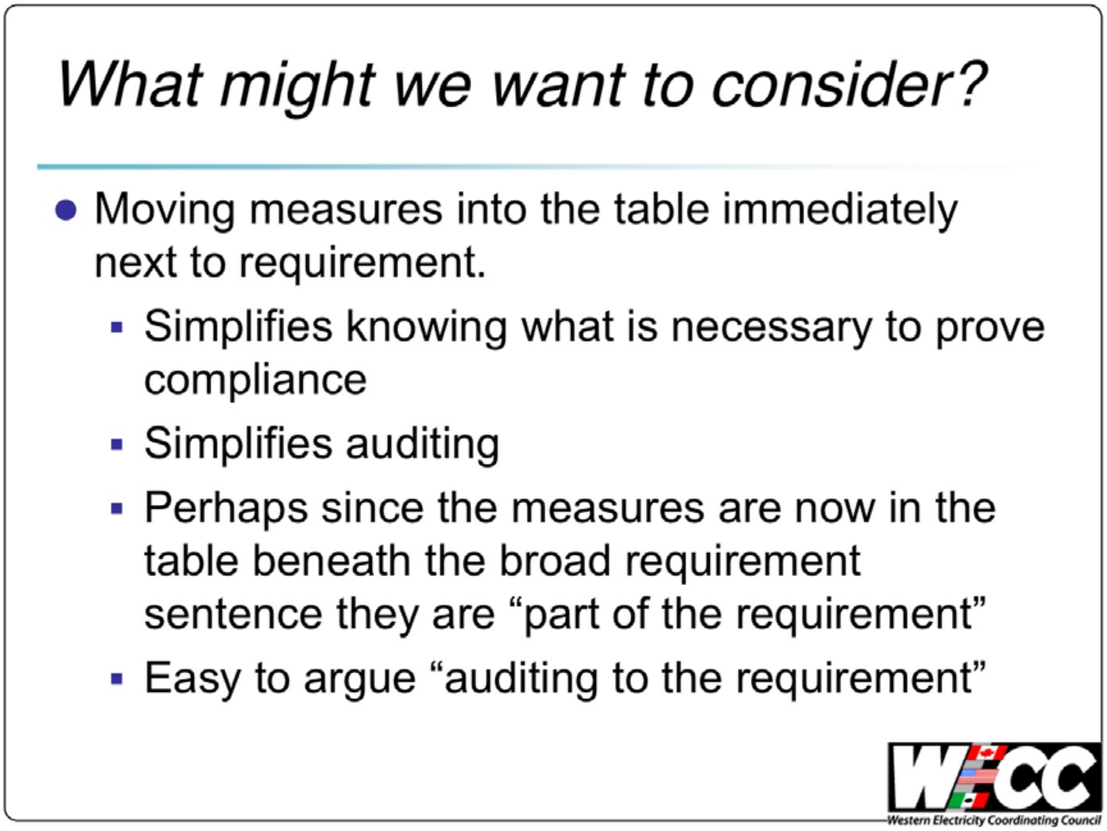
Supplemental Documents

- The PCI SSC has released several supplemental pieces of information to clarify various requirements. These documents include the following
  - Information Supplement: Requirement 11.3 Penetration Testing[5]
  - Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified[6]
  - Navigating the PCI DSS - Understanding the Intent of the Requirements[7]
  - Information Supplement: PCI DSS Wireless Guidelines[8]
- These are NOT referenced inside the standard and updated independently (might not be work for us because of NERC standard procedures ?)



What are we already using?

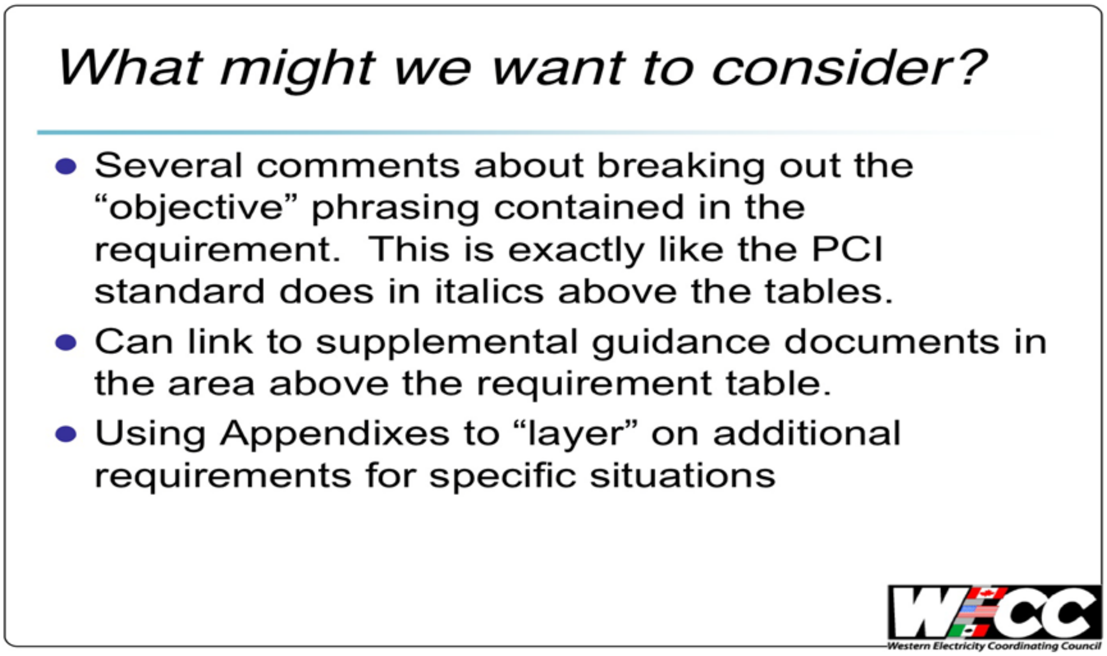
- Requirements grouped by Sections
- Broad simple requirement sentence is similar to current approach of generic requirement statement “in Table X…” above the table of specifics
- Table below broad requirement statement with specifics on how to achieve the requirement.



What might we want to consider?

- Moving measures into the table immediately next to requirement.
  - Simplifies knowing what is necessary to prove compliance
  - Simplifies auditing
  - Perhaps since the measures are now in the table beneath the broad requirement sentence they are “part of the requirement”
  - Easy to argue “auditing to the requirement”

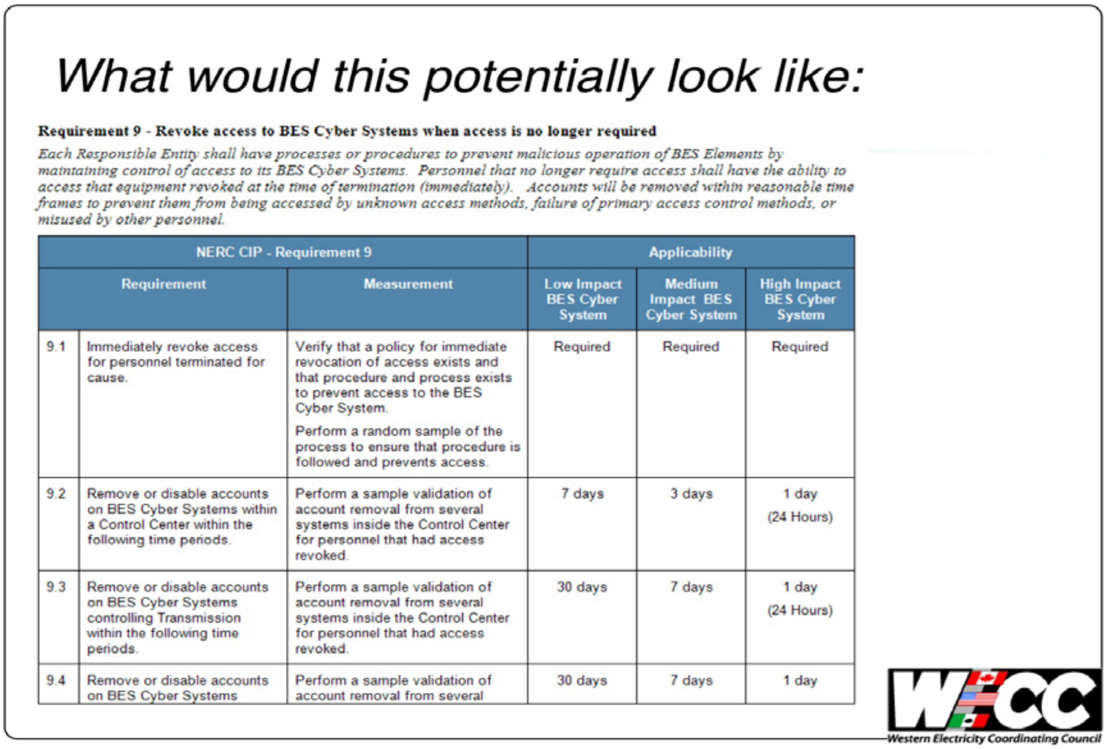
WECC
Western Electricity Coordinating Council



What might we want to consider?

- Several comments about breaking out the “objective” phrasing contained in the requirement. This is exactly like the PCI standard does in italics above the tables.
- Can link to supplemental guidance documents in the area above the requirement table.
- Using Appendixes to “layer” on additional requirements for specific situations

WECC
Western Electricity Coordinating Council



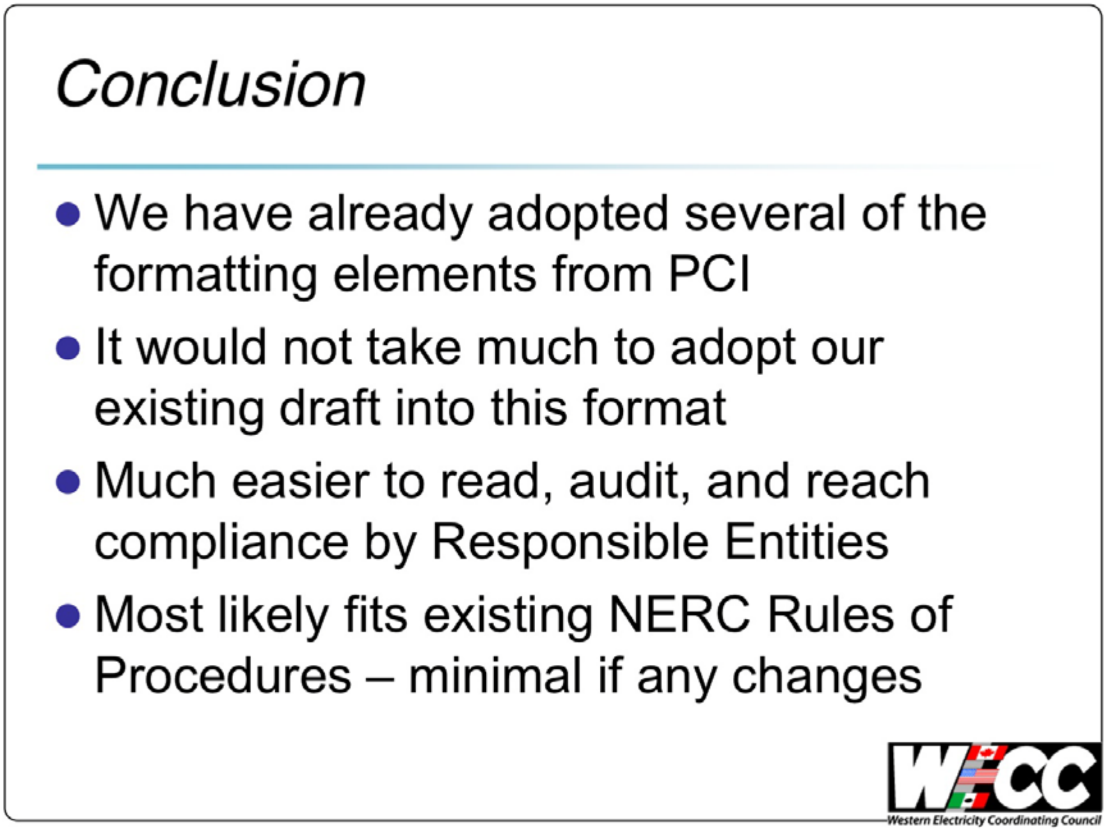
What would this potentially look like:

Requirement 9 - Revoke access to BES Cyber Systems when access is no longer required

Each Responsible Entity shall have processes or procedures to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems. Personnel that no longer require access shall have the ability to access that equipment revoked at the time of termination (immediately). Accounts will be removed within reasonable time frames to prevent them from being accessed by unknown access methods, failure of primary access control methods, or misused by other personnel.

NERC CIP - Requirement 9			Applicability		
Requirement		Measurement	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
9.1	Immediately revoke access for personnel terminated for cause.	Verify that a policy for immediate revocation of access exists and that procedure and process exists to prevent access to the BES Cyber System. Perform a random sample of the process to ensure that procedure is followed and prevents access.	Required	Required	Required
9.2	Remove or disable accounts on BES Cyber Systems within a Control Center within the following time periods.	Perform a sample validation of account removal from several systems inside the Control Center for personnel that had access revoked.	7 days	3 days	1 day (24 Hours)
9.3	Remove or disable accounts on BES Cyber Systems controlling Transmission within the following time periods.	Perform a sample validation of account removal from several systems inside the Control Center for personnel that had access revoked.	30 days	7 days	1 day (24 Hours)
9.4	Remove or disable accounts on BES Cyber Systems	Perform a sample validation of account removal from several	30 days	7 days	1 day

WECC
Western Electricity Coordinating Council



Conclusion

- We have already adopted several of the formatting elements from PCI
- It would not take much to adopt our existing draft into this format
- Much easier to read, audit, and reach compliance by Responsible Entities
- Most likely fits existing NERC Rules of Procedures – minimal if any changes

WECC
Western Electricity Coordinating Council

Appendix #10

CS0706 Standards Drafting Team
OVERVIEW OF UNOFFICAL AVERAGE OF RESULTS OF INDUSTRY COMMENT FORM POLLING

(120 SETS) JUNE 3, 2010

(Color Legend: Agree Disagree)

Combined average support for all sections (14) =51%

1. **Definitions 41% average section support**
2. **CIP-010-1 — Cyber Security 54% average section support**
3. **CIP-011-1 — Cyber Security — BES Cyber System Protection: 55% average section support**
4. **Security Governance and Policy (R1) 56% average section support**
5. **Personnel Training, Awareness, and Risk Assessment (R2 –R4) 43% average section support**
6. **Physical Security (R5 –R6) 40% average section support**
7. **Electronic Access Control (R7 –R14) 51% average section support**
8. **System Security (R15 –R19) 36% average section support**
9. **Boundary Protection (R20 –R22) 44% average section support**
10. **Configuration Change Management (R23) 50% average section support**
11. **Information Protection and Media Sanitization (R24 –R25) 64% average section support**
12. **BES Cyber System Maintenance (R26) 65% average section support**
13. **Cyber Security Incident Response (R27 –R29) 61% average section support**
14. **BES Cyber System Recovery (R30 –R32) 56% average section support**

Definitions 41% average section support

1.a. BES Cyber System Component
34 (31%)= Agree with proposed definition
76 (69%)= Disagree with proposed definition

1.b. BES Cyber System
30 (29%)= Agree with proposed definition
80 (73%)= Disagree with proposed definition

1.c. Control Center
42 (40%)= Agree with proposed definition
63 (60%)= Disagree with proposed definition

2.
67 (63%)= Agree with proposed definition
40 (37%)= Disagree with proposed definition

CIP-010-1 — Cyber Security 54% average section support

3.
49 (45%)= Agree with proposed definition
59 (55%)= Disagree with proposed definition

4.

66 (63%)=	Agree with proposed definition
40 (38%)=	Disagree with proposed definition

5.

41 (39%)=	Agree with proposed definition
64 (61%)=	Disagree with proposed definition

6.

62 (58%)=	Agree with proposed definition
45 (42%)=	Disagree with proposed definition

7.

72 (67%)=	Agree with proposed definition
35 (33%)=	Disagree with proposed definition

CIP-011-1 — Cyber Security — BES Cyber System Protection: 55% average section support

9.

48 (44%)=	Keep CIP 011-1 as one document
38 (35%)=	Break CIP 011-1 up into multiple standards
23 (21%)=	No Preference

10.

67(66%)=	Agree with proposed definition
34(34%)=	Disagree with proposed definition

Security Governance and Policy (R1) 56% average section support

11.

58(56%)=	Agree with proposed definition
46(44%)=	Disagree with proposed definition

Personnel Training, Awareness, and Risk Assessment (R2 –R4) 43% average section support

12.

23(23%)=	Agree with proposed definition
77(77%)=	Disagree with proposed definition

13.

59(60%)=	Agree with proposed definition
39(40%)=	Disagree with proposed definition

14.

43(47%)=	Agree with proposed definition
48(53%)=	Disagree with proposed definition

Physical Security (R5 –R6) 40% average section support

15.

37(40%)=	Agree with proposed definition
56(60%)=	Disagree with proposed definition

16.

37(41%)=	Agree with proposed definition
54(59%)=	Disagree with proposed definition

Electronic Access Control (R7 –R14) 51% average section support

17.

56 (58%)=	Agree with proposed definition
40 (42%)=	Disagree with proposed definition
18.	
66 (69%)=	Agree with proposed definition
30 (31%)=	Disagree with proposed definition
19.	
74(80%)=	Agree with proposed definition
19(20%)=	Disagree with proposed definition
20.	
45 (48%)=	Agree with proposed definition
48 (52%)=	Disagree with proposed definition
21.	
50 (55%)=	Agree with proposed definition
41 (45%)=	Disagree with proposed definition
22.	
27 (29%)=	Agree with proposed definition
67 (71%)=	Disagree with proposed definition
23.	
30 (33%)=	Agree with proposed definition
62 (67%)=	Disagree with proposed definition
24.	
27 (28%)=	Agree with proposed definition
68 (72%)=	Disagree with proposed definition
25.	
44 (46%)=	Agree with proposed definition
51 (54%)=	Disagree with proposed definition
26.	
47 (50%)=	Agree with proposed definition
47 (50%)=	Disagree with proposed definition
27.	
51 (55%)=	Agree with proposed definition
41 (45%)=	Disagree with proposed definition
28.	
49 (54%)=	Agree with proposed definition
42 (46%)=	Disagree with proposed definition
29.	
55 (60%)=	Agree with proposed definition
37 (40%)=	Disagree with proposed definition
30.	
50 (55%)=	Agree with proposed definition
41 (45%)=	Disagree with proposed definition
31.	
37 (40%)=	Agree with proposed definition
55 (60%)=	Disagree with proposed definition
32.	
31 (34%)=	Agree with proposed definition
60 (66%)=	Disagree with proposed definition
33.	
51 (58%)=	Agree with proposed definition
37 (42%)=	Disagree with proposed definition
34.	
49 (57%)=	Agree with proposed definition
37 (43%)=	Disagree with proposed definition

SYSTEM SECURITY (R15 –R19) 36% AVERAGE SECTION SUPPORT

35.
25 (27%)= Agree with proposed definition
67 (73%)= Disagree with proposed definition
36.
40 (45%)= Agree with proposed definition
49 (55%)= Disagree with proposed definition

BOUNDARY PROTECTION (R20 –R22) 44% AVERAGE SECTION SUPPORT

37.
28 (31%)= Agree with proposed definition
62 (69%)= Disagree with proposed definition
38.
49 (56%)= Agree with proposed definition
38 (44%)= Disagree with proposed definition
39.
38 (46%)= Agree with proposed definition
44 (54%)= Disagree with proposed definition

CONFIGURATION CHANGE MANAGEMENT (R23) 50% AVERAGE SECTION SUPPORT

40.
36 (41%)= Agree with proposed definition
52 (59%)= Disagree with proposed definition

41.
48 (58%)= Agree with proposed definition
35 (42%)= Disagree with proposed definition

INFORMATION PROTECTION AND MEDIA SANITIZATION (R24 –R25) 64% AVERAGE SECTION SUPPORT

42.
54 (58%)= Agree with proposed definition
39 (42%)= Disagree with proposed definition
43.
65 (72%)= Agree with proposed definition
25 (28%)= Disagree with proposed definition
44.
43 (49%)= Agree with proposed definition
45 (51%)= Disagree with proposed definition
45.
62 (75%)= Agree with proposed definition
21 (25%)= Disagree with proposed definition

BES CYBER SYSTEM MAINTENANCE (R26) 65% AVERAGE SECTION SUPPORT

46.
64 (73%)= Agree with proposed definition
24 (27%)= Disagree with proposed definition
47.
41 (48%)= Agree with proposed definition

45 (52%)= **Disagree with proposed definition**

48.

61 (74%)= **Agree with proposed definition**

21 (26%)= **Disagree with proposed definition**

Cyber Security Incident Response (R27 –R29) 61% average section support

49.

54 (61%)= **Agree with proposed definition**

34 (39%)= **Disagree with proposed definition**

50.

52 (60%)= **Agree with proposed definition**

34 (40%)= **Disagree with proposed definition**

BES Cyber System Recovery (R30 –R32) 55.5% average section support

51.

39 (46%)= **Agree with proposed definition**

46 (54%)= **Disagree with proposed definition**

52.

52 (65%)= **Agree with proposed definition**

28 (35%)= **Disagree with proposed definition**