NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

February 16, 2010 | 1:00 PM to 5:00 PM CST
February 17, 2010 | 8:00 AM to 5:00 PM CST
February 18, 2010 | 8:00 AM to 5:00 PM CST
February 19, 2010 | 8:00 AM to 1:00 PM CST

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

Joe Bucciero, Bucciero Consulting, LLC

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT February 16-19, 2010 Meeting Summary Contents

Cover.....1
Contents.....2
Executive Summary.....3

I. AGENDA REVIEW, WORKPLAN, UPDATES AND COMMUNICATION PLAN 9
A. Agenda Review 9
B. Review of Proposed Workplan Schedule.....9
C. Communications Plan Review.....9
D. Cyber Security Initiatives Update.....12

II. REVIEW OF INDUSTRY COMMENTS AND REFINEMENTS OF CIP-002-4 13
A. Reviewing Industry Responses to CIP-002-4 Comment Form Questions 13
B. SDT Points of Agreement and Disagreement in Refining CIP 002-4 46
C. Alternative Approaches for CIP 002-4 48
D. Small Group Review of Industry Responses to CIP 002-4.....56
E. CIP 002-4 Next Steps.....60

III. SECURITY CONTROLS REQUIREMENTS (CIP 003-009) GUIDANCE 61
A. Security Controls Requirements Sub-Teams Progress Reports 61
B. Drafting Guidance Questions for Security Controls Requirements Sub-teams 62
C. Additional Drafting Guidance Statements 65

IV. NEXT STEPS.....66

Appendix 1: Meeting Agenda.....*67*
Appendix 2: Meeting Attendees List.....*70*
Appendix 3: NERC Antitrust Guidelines *72*
Appendix 4: SDT Work Plan Schedule.....*74*
Appendix 5: Security Controls Requirements Drafting Guidance Principles and Statements.....*78*
Appendix 6: Security Controls Sub-Team Rosters.....*80*

CSO706 SDT FEBRUARY 16-19, 2010 MEETING
EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, John Lim welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines. The host Jim Brenton, a SDT member, welcomed everyone to the ERCOT facilities and covered logistics. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. On Thursday morning the SDT approved without objection the meeting summary for the January 19-22, 2010 SDT session in Tucker, Georgia.

Bob Jones reviewed the SDT workplan and schedule and provided an overview of an alternative schedule that Chair John Lim developed for the SDT's consideration. Mr. Lim noted that Gerry Adamski, NERC's standards director, contacted him and the Vice Chair late last week to discuss the schedule in light of industry concerns with going to ballot with CIP-002-4 separately from the balloting of the controls requirements standard. Following the meeting, the Chair put together a draft alternative schedule to address this concern which was cited by over 75% of industry comments and was raised in the February 9 SDT conference call to review trade association and regional meetings that discussed CIP-002-4. The new schedule is designed to give the SDT more time to address comments and prepare a better, more complete draft for formal posting later in the year. On Thursday, the revised schedule with a memo and Gant chart to be drafted for the Standards Committee's review was unanimously adopted by the SDT.

Mike Gent, former President of NERC and Vice Chair of the ERCOT Board, thanked SDT members for their work and noted that with at least three bills in Congress giving FERC more authority, we know we have to act even though there may be different visions of what doing the right thing means.

On Friday, Gerry Adamski, Director of Standards provided an overview of the Communication Plan that was circulated to the SDT at the conclusion of the Tucker meeting and after discussion with the SDT agreed to begin planning for an industry workshop in late Spring after the new CIP 002 and the controls requirements standards are out for review.

NERC Staff and members provided brief updates on related cyber security efforts relating to the Critical Asset and Cyber Asset Identification Process, a presentation on the Team's work at the ARC World Forum, a NERC bulk system policy statement, and NIST's release of a second draft of their report and a Cyber Shock Wave cyber attack exercise
The SDT reviewed industry responses to the Comment Form Questions provided with the preliminary draft CIP-002-4 standard for industry comment and discussed refinements of CIP 002-4. The Chair and Vice Chair proposed using the "points of agreement/disagreement/confusion table" that was started on Tuesday and asked members to

add any additional concerns as the Team reviewed the industry responses to Comment Form questions. The Industry Comment Form featured 13 questions and the Team received over 500 pages in comments. For most of the questions, there was a relatively low level of industry agreement with the proposals (between 20-40%). In preparation for the meeting, John Lim, Phil Huff, Howard Gugel and Scott Mix agreed to review the industry comments received in response to the Comment Form questions and provide the SDT with a review of the themes and a summary of the industry's comments. The full SDT reviewed the summary of industry comments, and later split into the following sub-teams to review and propose revisions to the CIP 002-4 standard based on the comments received: Definitions; Attachment #1; VSLs; Standards Requirements; and External Oversight.

CSO 706 SDT Points of Agreement, Disagreement and Confusion in Terms of CIP 002-4

Points of Agreement *regarding Industry Comments on CIP 002-4*	**Points of Disagreement *regarding Industry Comments on CIP 002-4***	**Industry Points of Confusion *regarding CIP 002-4***
1. Flexibility is needed but may or may not be included in today's language	1. What is the CIP standard trying to protect against?	1. Do you start with R1 and work through R3 or is there more flexibility possible in CIP 002-4?
2. Functions of BES need to be considered, but may not be clear in today's standard language	2. Should it be connectivity vs. impact assessment	
3.Some form of inventory will be needed regardless of approach	3. How extensive should the inventory be for each approach	
4. Any approach needs to result in a categorized list of cyber systems	4. The cyber system should inherit the categorization of the BES asset (indirect impact mapping) vs. basing the categorization on an assessment of the external and internal threats (direct impact mapping)	
5. The SDT is addressing a range of cyber systems at play in the real-time control and operation of the BES	5. There should be flexibility and third party oversight as to what equipment has a reliability impact on the BES	
6. Bright lines will help to simplify the implementation and compliance with the standards	6. Categorization should be based on threat/ reach/ connectivity	
7. Where ever possible, the SDT should seek to combine steps and simplify the approach	7. If we are using a compliance framework, we should stick with a CIP 003-009 structure	
8. We function in a compliance vs. a performance assurance framework.		
9. The standard should be designed so those implementing it know why they are protecting assets and systems.		

10.We are designing a compliance not a performance assurance framework		

The SDT Reviewed Alternative Approaches to CIP 002-4 including a categorization of BES cyber systems based on use of routable protocols. Dave Norton had circulated in advance of the meeting a proposal which suggested the categorization of BES cyber systems should be primarily based on use of routable protocols (threat/reach/connectivity). The following proposal was presented for the Team's consideration:

Categorizations of BES cyber systems based on the potential impact of their compromise through the use of routable protocols as attack vectors.

- **Control center routable protocol = high**
- **Generation plant/transmission substation = medium**
- **All else = low**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	6	**4**	**9**	**2**	**2.7 of 4**

Jay Cribb offered the following concept for ranking:

Cyber System Impact on BES →	high	medium	low
Connectivity ↓			
Routable	high		
Non-Routable	high		
Stand Alone	medium		

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	4	**13**	**3**	**0**	**3.1 of 4**

Stu Langton reviewed with the Team the difficult nature and complexity of the task at hand and reminded them that we will continue to have disagreements. He noted that the SDT has met all previous deadlines and will continue to work together to meet the upcoming deadlines. Consensus doesn't mean we have to all agree and that we can disagree sometimes – differences are okay – if 75% want to move on, then we will – we need the minority on different issues to hang in there and keep working with us.

Scott Rosenberger presented a revised proposal on Wednesday and spoke about risks presented by connectivity and the challenges in defining terms accurately.

"Include connectivity as a factor in the BES Cyber System categorization"
Revised Proposal: Matrix for Levels of Controls to Be Applied

BES (attachment #1 of CIP 002-4)	High	Med.	Low
Connectivity-Routable/Dial-up	High	High	Med.
Non-Routable	Med.	Low	Low
Not Connected	Low	Low	Low

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	12	**4**	**2**	**0**	**3.6 of 4**

Phil Huff offered the following successive proposals for testing acceptability related to combining Attachment #1 & #2 for the SDT to rank. The SDT reviewed and ranked three versions of the proposal, as follows:

1st Version Proposed by Phil Huff
Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed (the Criteria is the Span of Control).

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	2	**9**	**9**	**0**	**2.65 of 4**

2nd Version Proposed by Phil Huff
Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed. ~~(the Criteria is the Span of Control).~~

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	1	**11**	**6**	**1**	**2.6 of 4**

Revised Concept of Combining Attachment #1 and #2

On Friday morning, Dave Revill presented a concept of combining Attachment 1 & 2 that was discussed overnight by a group including John Lim, Phil Huff, Dave Revill, Rich Kinas, Patrick Leon, Joe Doetzl, and Dave Norton. He noted that under this proposal:

- Attachment 2 becomes more of a guidance document
- REs shall categorize the BES cyber systems by applying criteria in CIP 002 Attachment 1
- Changed ~~BES Subsystems~~ to BES Cyber Systems
- Changed Generation ~~Subsystem~~ in Attachment 1 to Generation facility.
- Move Attachment 2 to a guidance document to identifying what immediate affect on real-time operations means

This proposal combines Attachment 1 and Attachment 2 by tying the criteria in Attachment 1 to BES Cyber Systems that immediately (i.e., 15 minutes or less) affect real-

time operation. Attachment 2 is moved to a guidance document for identifying Cyber Systems that immediately affect real-time operations. (including the connectivity matrix)

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	8	**10**	**1**	**0**	**3.4 of 4**

The SDT reviewed and ranked the following related to the proposal above:

R1. As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize its BES ~~Subsystems~~ Cyber Systems ~~under its ownership~~ by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES* ~~Subsystems.~~ *Cyber Systems*. (*Violation Risk Factor: High*)

Attachment 1: Criteria for BES Impact Categorization of BES Cyber Systems
Cyber Systems that would immediately affect real-time operations for:

- Generation ~~subsystem facilities~~ with aggregate rated name-plate generation of 2,000 MVA or more.
- Etc.

Move Attachment 2 to a guidance document to identifying what *Immediate affect on real-time operations* means.

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	15	**6**	**1**	**0**	**3.6 of 4**

On Friday morning, the SDT discussed next steps regarding refinements to CIP-002-4 and the development of a response document for the industry's consideration. The Chair proposed and the members agreed that a subteam of 4-6 members would be formed to work on refining CIP-002-4 between now and the March meeting in Phoenix, where they would present a new draft standard back to the full SDT as well as a response document. The team may also continue after the March meeting to finalize these tasks.

On Friday, the Security Controls Requirements Sub-Teams (including Personnel and Physical Security, Security Governance, Recovery and Response, Access, Control and Auditing, Change Management, System Lifecycle and Information Management and Security Operations) reported on progress made since the Tucker meeting, reviewed a set of threshold questions and drafting guidance statements, and met in Sub-teams to work further on their efforts and agreement on next steps. The questions included:

1) How we are going to handle writing requirements that apply to 'BES Cyber Systems' rather than 'Critical Cyber Assets'?
2) At what level are we to write the requirements?
3) We've got to have some kind of ruling on the topic of compensating controls in a NERC

CMEP world.

4) We need a standard way to not only handle the difference in impact and environment (CC/Gen/Tran), but the difference in cyber system/device class.

Based on the SDT discussion, the following guidance statements were proposed to be added to those developed at the Tucker meeting:

- Requirements should apply to either (1) the BES Cyber System as a whole, or (2) components of the BES Cyber System. When a requirement only applies to specific types of components, describe those types of components to determine where component classes exist. Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.
- Sub-Teams should start with the CIP words and tweak if needed to include some DHS language. However, the "level" of the requirements text should be raised, if needed. Be specific, not prescriptive.
- Compensating Controls are not allowed. Need to write a "what" requirement, not a "how" requirement.
- As guidance, the focus should be on setting the level of controls at a level to avoid applying it to a device class, or explain why a control is being applied to a device class (e.g., general purpose platform vs. purpose built platform also, Part A of the TFE for a set of classes)

The Chair reviewed the progress made at the meeting and the need for the sub-teams to continue to meet between Austin and the Phoenix meeting to prepare draft language for the security controls for review by the full SDT. He also noted the agreement on a revised schedule by the SDT and the formation of a subteam to take the CIP-002-4 draft and make refinements and develop a response document to the industry's comments.

The Vice Chair agreed to work with the facilitators to revise the Sub-team drafting guidance statements based on this discussion and circulate them in advance of the March meeting.

The meeting adjourned at 12:15 p.m.

_____

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT JANUARY 19-22, 2010
AUSTIN, TEXAS

MEETING SUMMARY

I. AGENDA REVIEW, WORKPLAN, UPDATES AND COMMUNICATION PLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). 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 host Jim Brenton, a SDT member, welcomed everyone to the ERCOT facilities and covered logistics. The Chair reviewed the meeting objectives noting that focus of this meeting will be reviewing the industry comments received and discussing schedule forward – start drafting responses to comments following review and discussion of the schedule in response to comments and concerns from industry about addressing 002-4 separately from the rest of the standards. Phil Huff noted the intention was to consider the summary and full set of comments in small groups related to the questions posed in the comment form in order to develop general responses. He reminded the SDT that these are "informal comments" and we want to be responsive and keep the dialogue with industry going. Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the January 19-22, 2010 SDT session in Tucker, Georgia.

B. SDT Workplan and Schedule

Bob Jones reviewed the SDT workplan and schedule and provided an overview of an alternative schedule that Chair John Lim developed for the SDT's consideration. (*See Appendix #5).* Mr. Lim noted that Gerry Adamski, NERC's standards director, contacted him and the Vice Chair late last week to discuss the schedule in light of industry concerns with going to ballot with CIP-002-4 in late Spring and then separately later in 2010 balloting CIP 003-009. Following the meeting, the Chair put together a draft alternative schedule to address this concern which was cited by over 75% of industry comments and was raised in the February 9 SDT conference call to review trade association and regional meetings that discussed CIP-002-4 *(See Appendix #)*

Mr. Lim noted that this issue could put at risk the CIP 002-4 ballot without the remaining pieces being out for simultaneous industry review. The new schedule is designed to give the SDT more time to address comments and prepare a better, more complete draft for formal posting later in the Spring. It calls for informally posting an revised CIP-002-4 draft in March and by April begin to bring the security controls together with the CIP-002 governance standards.

SDT Discussion comments on the Schedule:

- Would a formal request for a second informal comment period need to be approved by the Standards Committee? Probably yes.
- The SDT needs to show progress but also be responsive to concerns from industry to see everything before agreeing to almost anything even in the informal comment period.
- Confused as to what is being proposed regarding the second informal comment period of CIP 002 and 003-009 controls schedule?
- Option to put 002 out for additional informal comment period or wait until other pieces are ready for combined informal comment period
- Posting for standards drafting team review by end of March (or April meeting?)
- CIP 003-009 ready for team review by March and finalized draft of CIP 002 – full package informal posting by April 19th
- The SDT is counting on time in March to prepare the security controls
- This is a slipped schedule – has FERC bought off on this? At the FERC/NERC meeting FERC staff acknowledged it might be problematic to put 002 out early and thought a combined posting made sense.
- CIP 002 is intended to determine bright lines of what to protect, not the how to protect it. Not sure we should say to people can wait until they see the how. This could lead to more gaming the system, what we are trying to get away from.
- People need the 003-009 security controls to understand the intent of CIP-002. Are we rushing to quickly through CIP 002 to get to CIP 003-009? Our schedule makes the assumption members have enough time to do this.
- Concerned about how the controls will match up with CIP-002 – the industry push back means they do not understand how the high/medium/low will work and fear that too much will be put in the high category. The schedule may be quick but not sure how else to do it.
- Early March post revised CIP 002 draft for comment to the SDT – remove “informal” to avoid confusion – FERC is going to wait until the whole package is ready to review. In order to meet end of the year deadline there is not much we can pull out of this proposed schedule – open to ideas for changes that would improve the product.
- Change “post” to circulate to avoid confusion
- The SDT members should be careful and avoid using “gaming the system.” The reality is that people are not sure what high/medium/low means and how controls will help define and be applied to each.
- We will not be ready to present the first draft of security controls at the March SDT meeting. Can present progress to review with full committee – this meeting we could focus and getting CIP-002 closer to completion.

- Taking CIP-002 off the table by June may help us to polish CIP002 but may take time away from preparing security controls. CIP- 002 is the most important piece to get right.
- It will be difficult to meet this proposed schedule– to have prayer of doing this we need to clarify common understanding of threshold questions across the sub-teams.
- Question for NERC standards committee? Communication with FERC regarding changes in the schedule?
- Be sure to look at the July period on – posting for three comment periods will require a lot of time for responding to those questions
- People are confused by the multiple sources requesting comments – series of rapid turnarounds may further confuse the industry
- Need to approve a new schedule? Review highlights and check on questions:
- In Austin – react to comments and develop consensus on 002 – start redrafting 002
- Sub-team meetings in next two weeks to refine 002 – by beginning of March have draft for full team review.
- Phoenix – finalize CIP 002 draft by end of first meeting day for posting/review but not comments – focus on sub team drafting of 003-009 controls.
- April 5th– have all control groups to have drafts for circulation to the rest of the SDT team as a package
- March in Phoenix: First draft of what? The controls? Should say draft CIP 002 for full team comment in Phoenix followed by team review of sub-team progress and drafts of sub team drafts of controls requirements.
- Present controls draft requirements for full team review and comment week of 4/12 followed by Sub-team refinements as needed in response.
- Posting of full package in May for informal comment
- May time period for a technical conference (face-to-face) or webinar with industry for review and comments?
- Should we think of a thirty day comment period allowing us to post May 1 with comments by May 31 – gives us time to work in sub teams through April – deal with comments/responses at the June meeting – everything following June stays the same
- Consider the mid-May meeting dates in Dallas for preparing for a technical conference to follow a week or two later.
- June SDT respond to comments.
- Series of ballot/comment periods in subsequent SDT meetings – formal comment periods require responses to each comment.
- Schedule allows for three comment periods if needed – can make changes to the draft based on the comments – allowed to keep the same ballot pool and deviate from required process to shorten periods required for re-balloting
- Need to verify assumptions in schedule with the Standards committee – Chair will take this forward.
- May need more time at the end to be sure prepared to file
- If make significant changes to the standard may impact those who need to be in the ballot pool

- Attach a draft schedule with a memo for the Standards Committee – put into a gant chart to show alignment?
- Review on Friday for adoption
- Schedule needed to meet requests is aggressive and will require people at this table to devote time and resources to make it happen – once approved we will be stuck with it

On Thursday the Revised schedule with a memo and Gant chart to be drafted for the Standards Committee's review was unanimously adopted by the SDT.

Mike Gent, former President of NERC and Vice Chair of the ERCOT Board, thanked SDT members for their work and noted the Team should blame him for some of this work. He also noted the facilitation team helped NERC in working with the Blue Ribbon Group in 1997-98 that lead the creation of the ERO. We wanted to be sure that the industry were effective without being too burdensome because doing nothing is unacceptable. While there may be different visions of doing the right thing and we are still not sure what we have to do, but know we have to do it. There are presently at least three bills in Congress giving FERC more authority.

C. NERC Update on Implementing the CIP Communication Plan

On Friday, Gerry Adamski, Director of Standards provided an overview of the Communication Plan that was circulated to the SDT at the conclusion of the Tucker meeting.

- Begin work on implementation in terms of industry outreach.
- NERC may produce a newsletter of which this would be a part as well as a maintained frequently asked questions list. For example the new concept of connecting CIP 002 with CIP 003-009 for industry review would be a good example.
- NERC also convened a meeting with FERC in January to review SDT progress.
- Need to hear more about the communication plan at a meeting soon
- The SDT Webinar on CIP 002-4 in late January was a helpful effort that had 475 registered and that members Jay Cribb and Sharon Edwards moderated and John and Phil joined in as well. There were many thoughtful questions – many of the concerns in the industry comments came out during the Webinar discussions
- Spent a lot of time explaining why the changes were needed
- The most heard comment involved the need to see CIP 003-009 before approving CIP 002
- They expressed they were used to the current system and hoped the SDT would build on it . They did not say it was necessarily the best system.

SDT Questions and Comments

- The team's adopted revised schedule will impact our communication plan.

- We need to communicate with a summary document our work on and with the informal comments – "post" the revised CIP-002 on website without soliciting industry comment and wait to marry this with the rest of the package of security controls.
- Consider an industry conference call to lay out the new strategy and schedule.
- Also consider an in-person face-to-face technical conference/workshop later in the Spring (Late May). This would take a lot of work and communication on NERC's part.
- Use the mid-May SDT Meeting to work on preparation for the workshop.
- Consider marrying the workshop up with the June team meeting in Sacramento?
- Need to get an updated copy of the communication plan to members so they can review and offer comments or suggestions.
- What would be the preferred location for the workshop? Connected to a SDT meeting? Near a central major airport?

D. Related Cyber Security Efforts:

NERC Staff and members provided the follow brief updates on related cyber security efforts:

- Scott Mix noted that the Critical Asset and Cyber Asset Identification Process comment period closes at the end of February. He noted there has been some confusion regarding these overlapping but distinct efforts and the closing of this process should help in that regard.

- Keith Stouffer reported on a presentation on the Team's work at the ARC World Forum much of the audience familiar with what is going on – aware of proposed expansion of scope of the standards – some worried it would seep down into distribution – anxious to see the final product.

- NERC is also coming out with a bulk system policy statement. It would be helpful to the Team to have someone from NERC provide clarification – may expand our understanding of the bulk electric system.

- Joe Bucierro noted that NIST has released a second copy of their report. He suggested that individual Team members may want to review and comment as appropriate. There also may be some point of coordination that the Team may want to consider going forward. Several Team members have been participating in the development of the report.

- Cyber Shock Wave was a bi-partisan policy group running an cyber attack exercise. Jay Cribb and other Team members were involved in helping write the scenarios.

II. SDT REVIEW OF INDUSTRY COMMENTS ON CIP-002-4

A. Reviewing Industry Responses to Comment Form Questions and Discussion of Refinements

The Chair and Vice Chair proposed to use the points of agreement/disagreement/confusion table (*see B.2 Below*) started on Tuesday and asked members to add any additional concerns as the Team reviewed the industry responses to Comment Form questions.

The Industry Comment Form featured 13 questions and the Team received over 500 pages in comments. In preparation for the meeting, John Lim, Phil Huff, Howard Gugel and Scott Mix agreed to review the industry comments responding to the questions and provide a review of the themes and a summary of the industry's response to CIP 002-4.

1. Comment Form Question #1 – Definitions

Scott Mix provided the overall summary for Question #1 from the industry responses for definitions of new or revised terms for possible inclusion in the NERC Glossary. These included: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact.

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification.

Overview of Industry Responses to Question #1 Definitions

General Responses.

- CIP 002-4 is still too complex / no clarity / ambiguous / vague
- Retain existing definitions – with clarification, don't reinvent the wheel.
- "BES" vs. "BPS" discussion – consistent across regions – 100kV bright line
- Proper use existing NERC Glossary definitions such as "Element", "Facility", "Adverse Reliability Impact", etc
- Need to see CIP-003 – CIP-009 to assess definitions.

Specific Responses

1.a. Cyber System Definition

1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

Option	Count	Percent
Agree with proposed definition	30	29.1

Disagree with proposed definition	63	61.2
Total:	**93**	**100.0**

Overview of Industry Responses to Cyber System Definition

- "Subsystem" adds unneeded step and confusion
- More clearly define "Subsystem" / "one or more"
- How do we determine what a "subsystem" is
- Routable and dial-able protocols – accessibility?
- Overly broad definition?
- What does "programmable" mean and where does it come in?
- Cyber "system" term may be unnecessary
- Add phrase "all components necessary to make BES function"
- Is this too vague?

SDT Discussion of Cyber System Definition

- Focus on Routable protocols, dial-up assets / connectivity / accessibility
- Mandate "testing" and "recovery"
- Why include "maintenance", "sharing", "communications", "disposing"
- This is an overly broad definition
- "Programmable" not defined – where programmed (factory or end-user?)
- This may be an unnecessary term – Consider using "Cyber Assets"
- Focus on real-time applications
- Does address "Non-cyber" cyber systems?
- Would encompass every cell phone, etc as a cyber system?

1.b. BES Cyber System Definition

1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Question 1.b. (99 Responses)

Option	Count	Percent
Agree with proposed definition	27	26.2
Disagree with proposed definition	72	69.9
Total:	**99**	**100.0**

Overview of Industry Responses to BES Cyber System Definition

- Add “also includes all components necessary to ensure the protection of the reliability functions being performed”
- Should refer to Attachment 2
- “Has the potential” is to vague
- Define “critical”, “adverse”, “degrade”, “compromise”, “critical functions”, etc
- Use “Adverse Reliability Impact” which is a defined term
- Use concept of risk
- No benefit over use of Critical Cyber Asset – use Critical Cyber Asset
- Remote accessibility
- Define the term, not the impact
- Capture “misuse”
- Change term to “Critical Cyber System”
- Change “has potential” to “has significant potential” – or change to “will”
- Accessibility issue (wired and wireless)
- Availability of asset impacts “potential to adversely impact” – is this what the SDT wants?
- Add “essential to operations” and “routable protocol”
- Relationship to NRC (nuclear) definitions
- Exclude market systems
- Change to “Cyber Systems controlling BES Facilities”

SDT Discussion Points of BES Cyber System Definition

- Need definitions of compromised, misuse, etc.
- No concept of risk or vulnerability?
- Retain CCA definition
- Change to critical cyber system
- Wired and wireless accessibility
- What about the concept of risk?
- Add essential to operations.
- Note the terms being used here versus those in use in nuclear industry
- Exclude market systems if that is what you want.

1.c BES Subsystem Definition

1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

Question 1.c. (95 Responses)

Option	Count	Percent
Agree with proposed definition	30	29.1
Disagree with proposed definition	65	63.1

Total:	**95**	**100.0**

Overview of Industry Responses to BES Subsystem Definition

- Define "BES Functions"
- Change to "Generic term for Generation Subsystem, Transmission Subsystem, and Control Center"
- Include "Protection Systems", "SPS', "RAS", "Automatic Load Shedding"
- Change "transport energy" to "transport electricity" -- or drop phrase
- Unnecessary – can use individual terms without loosing any meaning
- Define "shared element"
- We need to better define "BES facility." Break down into transmission, generation and control systems?
- "Transmit" electricity not transport energy
- Shared cyber and subsystems in generation subsystem
- We shouldn't' introduce the ability to decertify to meet compliance.
- Clarify "control system" versus "control room" concept – lack of definition causes confusion.
- Don't include the impact
- Misuse and decoupling causes bad behavior
- It is a open question as to where does generation ends and transmission begins.
- Change "output" to capacity
- Is "capable of" is overreaching?
- Change to "alarm processing"

SDT Comments on Question #1 First Round Responses, 1c. BES Subsystem Definition

- Potential agreement – h/m/l definition should be removed vs. tied to criteria –
- This misunderstanding cascades through the rest of the document.
- **BES Impact.** Support for a BES impact definition? – We need something in the glossary or in the text – but we should leave it at a very high level.
- Consider a BES impact clarification language in the preamble to this.
- Many comments refer to adverse reliability impact? Should we tie to that?
- Keep in mind that we will reference h/m/l in the controls too.
- Does defining BES impact add anything to common use or dictionary definition?
- Do we need BES impact? Already have adverse reliability impact and it covers the need (as read)
- There appears to be a lot of confusion in industry responses between BES cyber systems and cyber systems.
- Move into one definition – remove cyber system definition and collapse into single term of BES cyber system.

- Many of the respondents appear concerned with the subsystem definition and want it removed.
- **How Broad should the "Subsystems" Definition Be?** We have to be careful in responding to the comments– some may be understanding "subsystem" as a unit in a plant. Consider defining it better rather than removing it.
- Confusing topic – The SDT itself could not agree on how many subsystems there are in a plant.
- We do need a better definition – no one knows where this begins or ends – may need to get rid of it?
- Alternatively, we need to be more specific as to what we mean in the criteria.
- Need to better define rather than get rid of it – don't know how to clearly look at our assets as now written. It may be tempting to decouple systems which is not our intent.
- Perhaps use generation and transmission in distinguishing subsystems.
- If the SDT redefines this, we can not leave as a choice. We have to make it clear what a subsystem is.
- Need clarity, not throwing it out.
- If we create new definitions then we need to be clear what we mean – adding new layers doesn't serve anyone.
- Has to be clear for purposes of compliance – be clear or stay away from it.
- Security guidelines define common mode of impact – shared elements have cyber controls – has to be something we can make a difference on cyber security, otherwise we should not group together.
- If we cannot describe it sufficiently, then we need to drop it.
- Many of the comments indicate the subsystems definition was overly broad – can we all agree it should be more limited?
- BES cyber system is an effort to limit it to those impacting the BES system.
- Cannot look at transmission, generation and control systems without the other – can't start with just cyber system.
- Do we want to add back in the distinctions between routable protocol and dial up?
- Want protections over all cyber systems that may impact reliability and connectivity – but careful how we word this. Routable protocols may be easier to access and need higher level of control – but in the end it is about the controls we apply.
- What are we protecting? You can take out a substation and the BES will still function.
- Have not talked about the concept of protecting "data in motion" and how you that can be done.
- **Role of Controls in Handling Vulnerability.** Many industry comments on how to handle vulnerability, connectivity, accessibility to the system – do we handle it in the controls – is it a h/m/l or does it need to be addressed in the requirements?
- You don't put in either.
- Comments suggest we need to handle it – question is where do we best handle it?

- Industry concerned about removal of "routable" – are these critical infrastructure protection standards or cyber security standards? Cyber exists because of routable protocols – clarify which we are focusing on
- **Connectivity.** Putting protection on cyber system in a substation that does not have connectivity is not necessary.
- If BES is high then any cyber system associated with it may be swept in as high as well. We need a separate "if- then" determination of whether the related cyber system is high or not.
- **Categories vs. Risk Categorization.** Categories are impact only – they are not a risk categorization – we haven't come up with a risk categorization that can be audited -
- **N-1.** Propose adding into "disagreement" for discussion the N-1 concept
- "Individual field assets have intrinsically lower impact, on the basis of N-1 (planning?) engineering, than do control systems."
- Does N-1 matter?
- Intrinsically control centers are more important due to the manner we operate – to real time operations
- N-1 refers to credible contingency. There are many items not consider "credible" under N-1 that may still need to be considered in cyber security, e.g. transmission corridor failure is not considered "credible" –
- N-1 is important to planning but may not be to security of the cyber system.
- N-1 doesn't address intentional misuse. Instead is it about handling the largest single contingency?
- Is the 002 concept more succinct than N-1?
- Remove 'on the basis of N-1 engineering" – also change to "control centers" –Now move this up to points of agreement?
- BES is planned to a much higher standard than N-1 – if a transmission corridor is a common one, then contingencies are planned for – we are concerned with multiple external threats – if planning is not considered then you cannot identify the systems that need protection ahead of time.
- Cyber security for N-1 requires understanding the scope and reach of the hacker. This is not an apples-to-apples comparison.
- The way we engineer and operate the current system works. Thatmore accurately captures what I was trying to say than looking at it as N-1.
- Cannot build and design transmission systems for every contingency.
- Removed routable language at the direction of NERC to avoid perception of "gaming." Confusion in industry as to why this was removed is understandable.
- Careful about creating unintended consequences: e.g. airlines are now cancelling flights rather than risk fines for letting passengers sit in the plane on tarmacs too long.
- Need to look at mitigating risk from interconnectivity and from physical access.
- Make sure focus is on power system alarms.

SDT 2nd Round Discussion of Definitions- BES Subsystem Definition

- Need to clarify on the SDT as to what we are trying to protect against. E.g. protect against cyber attack that will impact the BES.
- However that leaves broad areas still open. We need to establish bright lines of potential threats and assure "graceful degradation" under a cyber attack.
- But how can it be measured in a compliance context rather than in a performance-based process?
- We can't prevent an attack, but we can design this so as to slow the attack.
- Cyber security – potential for hackers to attack and infiltrate bulk power system control and operations systems, such that assets could be damaged or misused in sufficient scale as to cause unacceptable outcomes for the BES.
- We need to design not just to address the attack potential, but also so we can avoid impacts due to negligence from within – not just attack vectors from outside.
- "Graceful degradation" as concept, how would it be measured?
- NERC definition– protect against rather than prevent.
- Minimize the impact of a cyber incident – including attack or misuse. We are trying to minimize the negative impacts regardless of internal or external, intentional or not. "Hackers" are not limited to external threats
- It is a term of art widely seen in industry as external and intentional – we need to protect from internal and unintentional too.
- Note the NERC definition includes the language in the paragraph before "cyber security" – includes minimize the risk.
- Still unnecessarily constrains the definition to outsiders with intentions. This does not even include current standards?
- Homeland Security definition? "Use sound risk management principles to implement physical and cyber protective measures that enhance preparedness, security and resiliency." (DHS)
- Maintain/preserve/assure reliability of the BES through implementation of generally accepted information system security practices (GASSP or GAISSP)

1.d. – Generation Subsystem Definition

1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Question 1.d. (89 Responses)

Option	Count	Percent
Agree with proposed definition	21	20.4
Disagree with proposed definition	68	66.0
Total:	**89**	**100.0**

Overview of Industry Responses

- Remove “shared element”, “shared cyber system”
- See glossary term- “Common Mode”
- Add “misuse”
- Opportunities to decouple systems as artificial behavior
- Define “Generating Plant”, “Generating Unit”, “Transmission System”, “Shared Element”, “Shared Cyber Asset”
- Clarify “Control room” vs. “Control Center”

1.e. – Transmission Subsystem Definition

1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Question 1.e. (89 Responses)

Option	Count	Percent
Agree with proposed definition	20	19.4
Disagree with proposed definition	69	67.0
Total:	**89**	**100.0**

Overview of Industry Responses

- Remove “shared element”
- Does “element” refer to glossary term?
- Don’t include impact
- Loss of multiple Elements may not impact reliability
- Add “misuse”
- Opportunities to decouple systems as artificial behavior
- Tie to registration requirements
- No bright line in the generation switch yard
- Add “one or more”
- “singular or in combination” – brings significant uncertainty
- Change “output:” to “capacity”

1.f. – Control Center Definition

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- 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 operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BES restoration activities.

Question 1.f. (92 Responses)

Option	Count	Percent
Agree with proposed definition	22	21.4
Disagree with proposed definition	70	68.0
Total:	**92**	**100.0**

Overview of Industry Responses

- Control room in a plant vs control center (or in a substation)
- "BES Asset" too vague
- Asset management includes commercial and market systems
- Change "of the" to "such as"
- "Capable of" is overreaching
- Change "alarm monitoring and processing" to "alarm processing"
- Define "BES Assets – or change to "BES Functions"
- Would include laptops and PDAs w/ SCADA client software – should only be fixed server locations and not remote clients
- Use actual configuration, not theoretical capability
- Define alarm to be "power system alarm", not fire alarm, etc
- Would bring into scope NERC RCIS, TLR, MISO outage scheduler, OATI, etc
- Data acquisition, aggregation, processing, etc too broad

1.g. – HIGH BES Impact Definition

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
  - BES instability; and/or
  - BES separation; and/or
  - a cascading sequence of failures.

  or
- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
  - instability; and/or
  - separation; and/or
  - a cascading sequence of failures;

or

- could hinder restoration to a normal condition.

Question 1.g. (94 Responses)

Option	Count	Percent
Agree with proposed definition	8	7.8
Disagree with proposed definition	86	83.5
Total:	**94**	**100.0**

Overview of Industry Responses

- 1st bullet – change to "that could directly and immediately cause"
- Add "unacceptable risk to IROL"
- Don't support 3 levels – add "no impact" – too complex or confusing
- Planning is not operations
- Does not match attachment 1
- Need to quantify "risk" – or remove "risk"
- Use "Adverse Reliability Impact"
- "prevent restoration" vs. "hinder restoration"
- Cranking path discussion
- Change "name plate rating" to MOD-024 requirements
- Don't need H / M / L definitions – use Attachment 1 instead
- "Unacceptable risk", "contribute to", "hinder", "planning timeframe" "degrade" is undefined
- Generation – use concept of capacity and time; differentiate base load units from peak units
- Not tied to mitigate vulnerabilities
- Restoration from blackout is not the same as causing / preventing blackout
- High impact Control Centers different than high impact transmission substations (transmission probably not high)
- Replace with "BES Impact" definition
- Use NERC event categories

1.h. Medium BES Impact Definition

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
  - directly affect the electrical state or the capability of the BES; or
  - directly affect the ability to effectively monitor and control the BES.

Question 1.h. (95 Responses)

Option	Count	Percent
Agree with proposed definition	11	10.7
Disagree with proposed definition	84	81.6
Total:	**95**	**100.0**

Overview of Industry Comments

- Refer to "High" definition comments
- Move 3 definitions to attachment 1 as a preface / corollary
- "affect the electrical state" too broad

1.i. Low BES Impact Definition

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not**:**

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

Question 1.i. (98 Responses)

Option	Count	Percent
Agree with proposed definition	15	14.6
Disagree with proposed definition	83	80.6
Total:	**98**	**100.0**

Overview of Industry Comments

- Reference back to High / Medium comments
- Change to "no impact"
- Add "no impact"

2. Comment Form Question # 2- Purpose of CIP-002-4

2. The Purpose of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement.

Question 2 (96 Responses)

Option	Count	Percent

Agree	27	26.2
Disagree	69	67.0
Total:	**96**	**100.0**

Overview of Industry Responses

- Only address real time operations
- Does not consider level or risk, e.g., remote access
- Need to consider CIP-002 – CIP-009 together; need to see CIP-003 – CIP-009
- Network connectivity
- Need a "no impact" category
- Effective date of standard toed to other standards (CIP-003 – CIP-009)
- Still a one-size-fits-all for cyber systems (inheritance issue)

SDT Discussion of Purpose

- Idea between 2 (asset based) and 3 (security based) are approaches to consider as either/or choice

3. Comment Form Question # 3-- Method of Categorizing BES Cyber Systems

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversly impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method.

Question 3 (82 Responses)

Option	Count	Percent
Prefer method proposed in the standard	46	44.7
Prefer alternative method of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1.	36	35.0
Total:	**82**	**100.0**

Overview of Industry Responses on Method of Categorizing BES Cyber Systems

- Need simplified criteria
- Flexibility to use either approach
- Must look at it both ways anyway for comprehensive approach
- Does not understand the question: standard does not say which way

- Use CIP-002-3 base, expand to BES assets instead of critical assets, apply R1.2 (list of asset types)
- "Cyber first approach" (using connectivity for categorizing): 8 entities support this approach.
- Need to know impact of CIP-003-009.
- "We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits."
- Hybrid approach: BES Engineering to filter out low impact subsystems and their BES cyber systems. For remainder, switch to cyber system approach and classify per "span of control" of BES assets.
- 2 dimensions of risk: BES subsystems and cyber systems (matrix approach)

SDT Discussion of Method of Categorizing BES Cyber Systems

- Not all the comments/responses are related to the question asked.
- Not intended to be a strict interpretation and not clear what is or is not captured in each – just a rough showing of confusion in the industry
- The question did not include "cyber first" as an option for consideration so we shouldn't give much weight to these industry preferences– again may just show there is no consensus for any one approach
- Merit to both approaches but each tackles a different aspect of what is needed – asset approach is appealing to get filter up front but may not capture all of the potential vulnerabilities – cyber first captures many of the vulnerabilities but without tying back to the assets.
- Hybrid approach – getting an inventory of every asset is immense and perhaps not necessary. The cyber impact was never intended to override the asset impact. If you have a high cyber impact but on a low impact asset, then it should still be a low category.
- Many utilities using CIP 002 to determine if they are meeting CIP 003-009 – Industry is worried about meeting CIP 002-4 process in terms of money and time only to find out they do not need to do much in CIP 003-009. We should provide entities an opportunity to understand up front as to whether they need to go through the whole process or not.
- Need to focus on the real attack vectors. For example, how many sites do we need to deal with because of routable protocols?
- **Combine Attachment #1 and #2.** Phil's proposed hybrid takes Attachment #1 and #2 and combines them to create a more bright line approach. The approach assumes it is criteria-based rather than the asset or cyber first approach – it also simplifies the current approach.
- The functions talk about what we are doing with the computers –may need to put this into the "disagreement" category because I am not sure I am comfortable yet with cutting out Attachment #2.
- Not sure there are not some unintended consequences with some of the terms used.

- This hybrid was intended as an example or starting point for further discussion and refinement.
- Still concerned about looking at cyber systems first before looking at assets. You would apply the same criteria. We need more detail added before adopting this as an alternative approach.
- This would simplify to a single requirement – makes audits simpler – impact based criteria – requirement is to list cyber systems that impact your high level assets (?)
- Inherited impact is addressed too
- Affects the risk rather than the impact
- Industry comments to the concept paper in the Fall were concerned with the complexity – so we removed the h/m/l of impact.
- Taking a leap that h/m/l of asset identification will identify the key cyber systems that need to protect the BES system.
- We cannot make the assumption but need to be careful in the scoping to mitigate the problem.
- Making the cyber system the subject of the sentence addresses the bulk of the comments from the industry – everything becomes high because of the physical asset – changing the subject here fixed that.

4. Comment Form Question # 4 Requirement-1 Responsible Entity Categorizes BES Subsystems

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems*.
1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that coulsd affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.
1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1."
Do you agree with this requirement? If not, please explain why and provide specific suggestions for improvement.

Option	Count	Percent
Agree	18	17.5
Disagree	75	72.8
Total:	**93**	**100.0**

5. Overview of Industry Responses to Requirement-1 Responsible Entity Categorizes BES Subsystems

- Need to know impact of CIP-003-009
- RCs should be removed from approval of engineering analyses
- Suggest Planning Coordinator for approval of engineering analyses
- Change within 30 days alternatives included: change to 30 days of being aware; change to 90 days; prefer annual reviews for changes; and any other change too broad: need better definition of this criteria
- Engineering analysis: need criteria for approval and consistency
- RCs and RAs should be required to publish approved engineering analyses
- General comments on vagueness of "subsystems"
- Blanket statement on engineering analysis (at front end of attachment 1)
- Subsystems it operates instead of owns. (joint ownership).
- Need explicit requirement for total list of subsystems.

SDT Discussion of Requirement #1- 1st Round

- Many people say they "disagree" even if they agree in order to get their comment read and considered
- **Owner/operator issue** – operating assets you don't own or own assets but don't operate them.
- Devices in the Texas interconnection system are owned by utilities by operated by regional entity
- The issue is who owns the cyber asset – they are responsible for the controls.
- Asset on site may be owned by the utility but operated by someone off site
- Need guidance from the NERC Compliance Group
- Add owner/operator issue to the agreement list for further discussion
- Even those who "agreed" often added suggestions for refinement or voiced concern
- Reviewed all the comments whether they "agreed" or "disagreed"
- **"Engineering assessment"?** How will we address those comments? Need a bright line approach.
- Draw bright lines but allow an option of an engineering assessment approach?
- FERC is not against exceptions, but must have appropriate controls and oversight of exceptions to ensure they are not misused.
- An engineering analysis could be used to either opt out as an exception or to opt in for units that are deemed to be critical.
- Need a way to allow an entity to declare something for a higher level protection without requiring a full analysis.
- What we are protecting against may need to be clarified for any review of the underlying analysis. Are we protecting against a single point or multiple point of attack?
- NERC was concerned with opt out, not with opt in

SDT Discussion, Requirement #1 - 2nd Round

- Needs more discussion – I think cyber approach takes more – I don't believe this discussion is worthwhile
- Is this a disagreement we need to reach a conclusion on now? Remove from list?

5. Comment Form Question # 5 -Requirement-2 Notification Proposal and Approach

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem:

2.1 Description of the Generation Subsystem that includes Facility designation(s), or name(s), location,
and other identifiers needed to identify the Facility(ies)

2.2 The Responsible Entity name

2.3 The BES impact categorization level"

Do you agree with this notification proposal and approach? If not, please explain why and provide specific suggestions for improvement.

Question 5 (86 Responses)

Option	Count	Percent
Agree	39	37.9
Disagree	47	45.6
Total:	**86**	**100.0**

Overview of Industry Responses- Requirement-2 Notification Proposal and Approach

- Define directly interconnected
- Change Transmission subsystem owners to transmission owners and operators
- Include method of notification and date of notification
- The same burden for information sharing should be placed on the Transmission Operators/Owners
- How does the GO/GOP know who his transmission owner/operator is? (He must connect to it?).
- Must be signed by Senior Manager
- Purpose of requirement not generally understood, must clarify and be more direct.
- Information protection issues

- Prefer annual requirement
- Address jointly owned facilities with different assessments (in attachment 1?)
- Several comments where allusions are made to the Transmission Subsystem owners categorize the Generation Subsystems.
- Modify CIP-002-3 approach
- RCs should categorize Generation subsystems – wide area view

SDT Discussion Requirement-2 Notification Proposal and Approach - 1st Round

- Annual requirement – if impact is changing frequently and have to continually reassess then put in the requirements – For audits do we have to determine or fix the point in time? Otherwise trying to do it in real time?
- Who doesn't know who their interconnect agreements are with? Have to have an interconnect agreement – how can you not know who the transmission owner/operator is?
- If you have joint ownership and they assess it at different levels, which applies? The higher assessment? Need to clarify

SDT Discussion of Requirement-2 Notification Proposal and Approach 2nd Round

- General agreement, but need to work on this as a team activity to see if it is possible. The language here is offered as an example.
- Adding "controlling/monitoring/alerting/protecting" is the key addition to the existing language
- "Unless it has been determined … {by} engineering evaluation…" are the opt out or weasel words that FERC is trying to get rid of – first part of the sentence is the bright line with the second part suggesting that you don't really have to meet the bright line. This paragraph is at cross purposes with itself.
- And RC/RAs don't want to do this.
- However there is no science behind the number offered here as the bright line.
- Alternative criteria for categorizing these?
- There should be no opt-out from a high but there could be an opt-up from medium or low approach – determined by an engineering assessment to be a high?
- May need to have a way to opt-down but not opt out .
- Assuming we are trying to drive issue to something the SDT can rank or shape for small groups to work with?
- I heard this as a suggested compromise approach to simplify R1 and R3.
- We cannot assure the bright line is correct and need to offer a way to address if it is not right for all entities in all situations.

- Change from "BES subsystems" to change the subject of the sentence to be "BES cyber subsystems."
- No bright line can cover all situations – must have an exceptions process available.

6. Comment Form Question # 6- Requirement-3 --Assigning Highest Impact Level of Associated BES Subsystems.

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows:

3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.

3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."

Do you agree with this requirement of assigning the highest impact level of the associated BES Subsystems? If not, please explain why and provide specific suggestions for improvement.

Question 6 (90 Responses)

Option	Count	Percent
Agree	36	35.0
Disagree	54	52.4
Total:	**90**	**100.0**

Overview of Industry Responses Requirement-3 --Assigning Highest Impact Level of Associated BES Subsystems.

- Attachment 2 is overly broad in scope or worse, open-ended.
- Specifically, situational awareness can incorporate just about any cyber system. The SDT should review each Reliability Function to determine what is in/out of scope.
- The focus should be on real-time systems or those that can cause an Adverse Reliability Impact as a result of compromise (as opposed to those cyber systems that provide a maintenance, planning, or other non-essential function).
- The focus of Attachment 2 should NOT be on what can compromise these functions but the adverse impact if these functions are compromised (i.e. Attachment 1). Rename the attachment to "Activities Performed to Maintain the Reliable Operation of the BES."
- The size/rating of a "BES Subsystem" (whatever that is – say, for sake of discussion, a substation) has no logically valid correlation with the degree of potential severity of adverse impact on BES reliability resulting from compromise of its associated cyber assets. The impact of the Cyber System should be taken into account first. A system

may pose LOW impact to its associated BES Subsystem but HIGH impact to a control system on the basis of being connected using a routable protocol.

- Categorization should take into account both the functions and BES Subsystem impact to determine the true impact category (i.e. bring back the categorization lookup-table that combines BES Subsystem and BES Cyber System impact categories). BES Cyber Systems associated and having the potential to impact BES Subsystems could create a "race to the top" and make everything High impact. Not all associated Cyber Systems will have High impact. For example, the pH monitor or ambient air sensor for a Generation Control System should not inherit the same category as the Generation Subsystem. Other factors to consider include:
  - the role of the BES cyber system within the broader context of the operation of the BES subsystem (Is this the only mode of failure of the BES subsystem?);
  - the technical capabilities of the cyber system (Does it provide information sensing capability or interactive control?)
  - the nature of the network that the interconnected BES cyber system is using (IP or serial); and
  - the connectivity if any outside a BES sub-system (Is remote access allowed?); are examples of the factors to consider.
- Redundancy (often mandatory requirements in other reliability standards) should be considered as it may reduce the impact of an individual BES Cyber System component. Redundant systems with different architecture or modes may require a lesser degree of security controls due to an inherent robustness, determined through a vulnerability assessment. Master ends of BES Cyber Systems may be categorized higher than the individual remote ends of the BES Cyber Systems, but no higher than the associated BES Subsystem.
- The categorization should take risk into account instead of just impact. Many comments equated this to taking remote accessibility into account when assigning a category. Others cited non-routable protocols as part of the risk equation. Still others called for a broader risk assessment.
- It is sufficient that the BES systems are assessed to have an impact. The degree of an impact is superfluous.
- Categorization should be addressed as part of the Security Controls.
- Need some guidance on identifying Cyber System components.
- Only High and Medium impact Cyber Systems should be identified since Low impact Cyber Systems do not have impact to the reliability of the BES; or since BES Cyber Systems would default to Low, there is no reason to specifically categorize them as such.
- We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.
- It should be clear that an entity cannot be found in violation of R3 given an omission of BES Subsystems in R1.

- Recommend that additional asset categories be addressed as well (i.e.: PSP, ESP, non-critical cyber assets, access control, monitoring, etc.)
- Attachment 2 should be placed in a guidance document.
- Why move away from Critical/non-critical? If the Cyber Systems pose little risk to the BES, then why spend significant resources protecting them?
- Need a timeframe for adding Cyber Systems to the list after identifying or recategorizing BES Subsystems. The CEMP could require an immediate change to the BES Cyber System as listed.
- It is not clear how firewalls, routers, HVAC and other supporting systems would be classified.
- Remove the explanatory text at the beginning of Requirement 3. It does not add anything.
- There should be a 4th, *no impact*, category.
- In order to support compliance activities, add the following and update the Measures section appropriately: R3: add text to require that the documentation created when categorizing and subsequent documentation called for in R3.1 & R3.2 to be signed and dated (by proper personnel identified per CIP-003 / R2).

SDT Discussion of Requirement-3 --Assigning Highest Impact Level of Associated BES Subsystems- 1st Round

- Possibly grouping the controls for organizational (process and procedure issues) or better definition of the low level of controls
- Or are they included in the low impact level – trying to address concerns regarding the burden of inventory
- A category of 'no impact" and do I have to then have to have a spreadsheet that documents everything else? Concerned how auditors will treat such a category
- Low by definition could include the "no impact" assets – like having criteria that better defines the "low" category
- Auditors should focus on the high and medium categories – the low left to the entity to secure as they see fit

SDT Discussion- 2nd Round

- Is it the data/information sharing or the network? What is the scope of the comment?
- Revisit later – in the scheme of issues, it is not vital at this point
- It is a possible attack vector – if not included, then it becomes the attack vector

7. Comment Form Question # 7 Proposed Violation Risk Factors and Violation Severity Levels

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Question 7 VRF (66 Responses)

Option	Count	Percent
Agree with VRFs	32	31.1
Disagree with VRFs	34	33.0
Total:	**66**	**100.0**

Question 7 VSL (68 Responses)

Option	Count	Percent
Agree with VSLs	20	19.4
Disagree with VSLs	48	46.6
Total:	**68**	**100.0**

Overview of Industry Responses on VSLs and VRFs

Broad VSL Responses

- Concerning VSLs, we recommend replacing zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented, program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented, high-controls not implemented, moderate-reviews not completed, lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
- We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case. Categorization of BES cyber systems and subsystems are an administrative process and do not present a high risk to the BES. Therefore it should have a low VRF; however, improper application of security controls might increase the risk to the BES.
- There needs to be VRFs for Transmission Operators and Reliability Coordinators not providing information to Generator Operators as required in Attachment 1 Sections 1.1, 1.2, 1.3, 1.4, 1.6 and 1.13.
- The requirements must be made much clearer in order to make the assessment of the appropriate level of VRFs.

- We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
- Moving from a Moderate to a High to a Severe due to a set period of time passing (10 days) is not consistent with the current implementation of VSLs and VRFs. The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed.
- VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here.
- Paradoxically, un-categorized BES subsystems or cyber systems must be categorized prior to VSL determination. Once they are categorized, the violation has been fully mitigated.
- Disagrees with the VSL level determinations due to the ambiguity associated with the high, medium and low categories.
- How will the number of "true" categorization or number of subsystems be determined as the basis of measuring what missed or mis-categorized? This severity level determination is far too reliant on an external judgment. The measurement needs to be absolute an unambiguous.
- Low impact BES subsystems have no effect on the BES and should not be in the violation security levels.
- Given the degree of subjective judgment that is involved with the categorization, it seems inappropriate to assess such a severe violation level for what could amount to a disagreement between the Entity and the Auditor on the Impact of a particular BES subsystem. Perhaps the VSL's should be based upon the completion or failure to complete a categorization exercise itself.
- The VSLs refer repeatedly to not categorizing a BES Subsystem of some impact level. Yet, without the categorization having taken place, how can the impact level have been determined? Also, the VSL refers to mis-categorized Subsystems. Who determines that the Subsystem was mis-categorized? Will the Regional Entities be performing their own independent categorization?
- Utilizing numeric values to change the VSL seems inappropriate when there may be wide variances in the quantity of BES Subsystems.

Specific VSL Responses

- R1 – Should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
- R1 – Moderate VSL should specify 31 to 60 days, and high VSL should specify 61 to 90 days, and Severe VSL should specify greater than 90 days to remain consistent with R2.
- R1 – Failure to update documentation should not carry the same weight as not categorizing any BES Subsystems.

- R1 - We suggest “One to three Medium Impact BES Subsystems have not been categorized or have been mis-categorized as Low Impact.” Then updating Moderate VSL to “Three or more Medium Impact BES Subsystems have not been categorized or have been mis-categorized as Low Impact.”
- R2 – make the timeframes consistent with the expectations in R1. 30-40, 41-50, 51-60. We require the Responsible Entity to update the list in these timeframes but do not require the Generator Subsystem owner to report the change in like timeframes
- R3 – the VSLs have gaps. For example in the Lower level, there is no violation if 1-4 BES Cyber Systems have not been categorized. There needs to be full coverage for all violations of the requirement to be consistent with NERC and FERC obligations. The other levels have similar issues. A remedy could be to assign impact levels based on the number of BES Cyber Systems not categorized (1 for Lower, 2 for Moderate, 3 for High, More than 3 for Severe)
- R3 (Moderate) – should reference BES Cyber Systems, not BES Subsystems.
- R3 – if a non-affiliated BES subsystem owner fails to correctly categorize its BES subsystem leading the Transmission Subsystem owner to assign too low a categorization to its cyber systems, then it may lead the Transmission Subsystem owner to incorrectly categorize its associated cyber system. Assigning a severe VSL to the Transmission Subsystem owner under these circumstances is inequitable.
- R3 – Moderate VSL: Add “Cyber” after “BES.” Per the current R3 VSLs miscategorizing 1 or 2 Medium Impact BES Cyber Subsystems will NOT result in a violation. The suggested change to R3, Lower VSL above will solve this issue. Severe VSL: The last sentence states “The Responsible Entity does not have a list of ALL its BES Cyber Systems.” Technically this means if the entity misses listing even one of its Low Impact BES Cyber Systems they would have committed a severe violation. Suggest changing “all” to “any.”
- The Violation Severity Levels appear inconsistent by equating a missed deadline for updating the categorized BES Subsystem list, with not categorizing any BES Subsystems under the Severe Violation Severity Level. All the deadlines for the VSLs should be 30 days, with differences based on impact level categorization. R1 Lower VSL should include “The Responsible Entity has failed to update its categorized list of Low BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the Moderate VSL should be changed to “The Responsible Entity has failed to update its categorized list of Medium BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the High VSL should be changed to “The Responsible Entity has failed to update its categorized list of High BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the R1 Severe VSL should be removed.
- The quantity thresholds used in the Violation Severity Level table should be a a weighted score of an entity’s subsystems, where multiple Low BES Impact Subsystems

or BES Cyber Systems are considered equivalent to single High Impact BES Subsystem or BES Cyber System, respectively.

SDT Discussion VSLs and VRFs

- Comment suggesting a different path for VSLs?
- EEI representative clarified concern – the bar should be a little higher and performance based.
- Add a more succinct version of the comment to the list.
- Consciously chose not to penalize entity for one-time violation of requirements in drafting the VSLs.
- True for medium but not high which is seen as severe.
- May push entities to high to address audits?
- Revisit the low level of VSLs with regard to zero based quality instead of zero based defect (see, EEI comment)
- Absolute perfection is the low bar –that is how the compliance system works – 99 out of 100 still fails

8. Question # 8 Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria? Suggestions for improving proposed criteria:

Overview of Industry Responses- Proposed Criteria-High, Medium, Low BES Impact Categories

- What is the basis for the bright line criteria (e.g. 2000 MVA/1000 MVA)?
- Must run: that have wide area impact
- Definition of Medium Impact is too vague
- More precise terms
- Criteria for the classification of Facilities for High, Medium or Low BES Impact should be based on the risk (probability and consequence) of one or more events that may cause an Adverse Reliability Impact, such as an event that may cause an IROL to be exceeded or cause a supply / demand mismatch greater than a certain metric such as the Contingency Reserves of a reserve sharing group (or another metric determined by study in the region).
- Bright line thresholds (such as 2000 MVA or 2000 MW) are useful default values that should be used in the absence of a particular BES design value used in a region for planning studies and real-time operations.

- The entire Attachment 1 can be boiled down to two metrics: supply / demand mismatch and IROLs.
- The categorization of black start units and transmission cranking paths between the black start units and the units to be started should be those identified under EOP-005-2 and based on approved region-wide restoration plans developed under EOP-006-2. As discussed earlier, "High Impact" from a restoration perspective should focus on preventing restoration efforts and "Medium Impact" should focus on hindering restoration in accordance with the regional plan. Hence, High Impact should be for a Cyber System that, maliciously used, could prevent black start efforts from multiple black start units and their cranking paths in the regional plan. Medium Impact should be for Cyber System that, maliciously used, could hinder black start efforts from a single black start unit or cranking path in the regional plan. Black start capable units that are not in the regional plan should be Low Impact.
- Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. (Generation?)
- Request clarification on the wording "leaving" in 1.5. Alternatively, suggest 1.5 be made to read: Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station…
- Restoration paths and UFLS: distribution facilities in scope?
- Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both?
- Remove Engineering Analyses.
- Blanket Engineering analysis opt-out in Attachment 1
- Exceeding an IROL does not cause instability if recovered within the timeframe allowed by the current standards requirements, and therefore should not be a H or M criterion

SDT Discussion = Round 1 Proposed Criteria-High, Medium, Low BES Impact Categories

- Role of transmission planning – industry wants it in and NERC is saying do not put it in
- Should we have engineering assessment opt outs?
- As applied to attachment one, struggled with the target number – agree we need to put it in even in the face of the directions from NERC
- Need to have it in there – up to the team, not NERC
- Seems clear to me that NERC does not expect to allow opt outs
- Moving to bright line gives a different framework than Commission considered when giving us guidance
- If there are exceptions to the requirements then need to be sure there is an accountability process
- May need an external party to review whether or not the rationale for the exception is appropriate

- Engineering assessment needs oversight – question would be who is willing to accept the responsibility?
- Still waiting for RAs to be designated – needs to be some entity to perform independent evaluations – may need to hold harmless from liability
- RAs are a renaming of RROs – version 4 document was approved a year ago December but the document was never brought to the Trustees for approval – version 5 is now on track to go before the Trustees – thus RA still not an official or legal standing and so no one has signed up yet
- 706 gives same protection that is granted to NERC –
- this is for telling you what assets need to be under the standards – can't just mark everything as high without documentation
- Should be discussing the validity of engineering assessments rather than who should do it – should we allow and if so, then discuss who and how
- We disagreed with having the engineering assessment as adding a layer of complexity – we are comfortable with the process we already have
- Opt out option seems to be contrary to the grouping of assets into the h/m/l buckets without adding value – create bright lines, but they don't really matter
- If we do not allow then saying bright line is absolutely correct for every entity across the country – irresponsible not to include
- The requirement is for "impact analysis" – throwing a number out there is not a true impact analysis – without exception then consider changing to "wild guess analysis"
- There is no right answer as to where to put the stake for analysis – what are we protecting against?
- Need to lock in what criteria will be used by a third party – not looking to except specific assets
- Have to have someway, with rules around it, to address changes – you can choose the bright line or if you choose an alternative then show us why and how
- Engineering analysis is use in two ways in the requirement
- Do we need a study to help set the criteria for the bright line?
- Can't possibly study all the possible situations across the country – put the burden on the entity seeking the exception to prove it is entitled
- NERC has bright lines in other standards without definitive analysis
- Who is the right organization to further study the issue?
- Leaving unspecified in the standard leaves it open to allowing anyone to do that – need to designate

SDT Discussion Round #2- Proposed Criteria-High, Medium, Low BES Impact Categories

- Added to the list for further discussion

9. Comment Form Question # 9 Attachment 1 High, Medium, Low BES Impact Categories for Load-Serving Entities, Transmission Providers and Interchange Coordinators.

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?

- Suggested Criteria for Load Serving Entities:
- Suggested Criteria for Transmission Service Providers:
- Suggested Criteria for Interchange Coordinators:

Overview of Industry Comments- Attachment 1 High, Medium, Low BES Impact Categories for Load-Serving Entities, Transmission Providers and Interchange Coordinators.

- The vast majority of responders had no suggested criteria for these entities.
- In fact, most felt that these entities should not be included as responsible entities in this standard.
- Those that felt that they should be included added that it depended on whether they had BES Cyber Systems.
- Some expressed that the systems were covered under other REs (Distribution Providers, TOPs, BAs)

SDT Discussion – Round #1 Attachment 1 High, Medium, Low BES Impact Categories for Load-Serving Entities, Transmission Providers and Interchange Coordinators.

- Does the definition even apply to the commenter?
- Possibly – may need to modify the language to clarify who it applies to.
- Demonstrates the folly of this approach – all of us are interconnected through the NERC net.
- Proper controls deal with that issue.
- DOD cannot fully protect its system, how can we?
- If we can't think of an instance where an entity should be included then it probably shouldn't be
- Review the registration criteria for including LSEs, TSPs and ICs under the CIP standards (if any)? If no criteria, then remove.

10. Comment Form Question # 10 Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories for NERC and Regional Entities

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities?

- Suggested criteria for NERC and Regional Entities:

Overview of Industry Responses Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories for NERC and Regional Entities

- The only responders that felt these entities should be included said that NERC Net was probably the only concern.
- Several felt that even NERC Net would not affect the BES.

SDT Discussion Round #1 Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories for NERC and Regional Entities

- NERC Net could be an Achilles heel if not properly protected
- We can't protect against the whole world – then every cell phone is an attack vector.
- The requirements around NERC and the regional entities are more stringent than the standards – and a better venue for addressing the information security issue – different audit regime by an outside third party entity
- NERC and regional entities were included in the CIP 002-4 draft – should they be? If you can create criteria, then yes. If cannot create criteria, then no.
- NERC alerts could affect the BES.

11. Comment Form Question # 11 Functional Entities- Distribution Provider and Reliability Assurer.

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities?
    - Comments on adding Distribution Provider:
    - Comments on adding Reliability Assurer:

Overview of Industry Responses- Functional Entities- Distribution Provider and Reliability Assurer.

- Most responders felt that the Reliability Assurer could be excluded (pointing to the fact that the RA is not included in the NERC Glossary, and confusion over how compliance for NERC and Regional Entities could be measured).
- Results for the DP were mixed. Some felt that the DP could be excluded, since they did not involve facilities >= 100kV.
- Some felt that the DP should be substituted for the LSE.
- Some were unsure how load shedding and Smart Grid would affect this standard.
- Some were very opposed, feeling this opened distribution up to FERC regulation.

SDT Discussion Points Functional Entities- Distribution Provider and Reliability Assurer

- RA could be excluded – what BES can they be connected to?
- Careful about distribution provider based on registration criteria – includes the wires company, most of whom are not registered – be cognizant of what the registration criteria calls for and who is actually registered

- Term bulk power system – reviewed language – does not include local distribution of electricity
- Under frequency load shedding – applicability – may need a long list of applicability to be sure capture entities we want to see in and not those we do not
- Do RAs have cyber systems that should fall under this standard?
- Frequency load shedding is a design standard, not a performance standard

12. Comment Form Question # 12 Attachment 2 Functions Critical to Reliable Operation of BES

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions?

- Suggestions for improving proposed functions:

Overview of Industry Comments Functional Entities- Distribution Provider and Reliability Assurer.

Broad Comments- Attachment #2

- The focus for these proposed functions should be cyber systems that support real-time operations.
- How are Attachment 2 functions different than the functional model? The standard already covers the assignment of applicability to functional entities and restating the tasks performed by the functional entities seems redundant.
- Does not indicate the varying levels of impact for the defined functions. This is a one-size-fits-all model for Cyber Systems associated with BES Subsystems.
- Attachment 2 is not careful as to whether it applies only to BES Elements. If it is taken to apply to any Element then it becomes a definition of the BES Subsystem.
- Make the list complete. The “include, but are not limited to” open ended function list leaves too much room for disagreement. Clearly identify if for each function if you need all of the elements below it or just one, to be considered having that function. For example if all you have is power system stabilizers, do you have the Dynamic Response function?
- Attachment 2 only adds confusion and should be eliminated.
- Attachment 2 supports the identification of cyber systems that support critical BES functions but seems to suggest by the title of the attachment that all functions being critical are also high impact and therefore does not assist with the categorization of assets that could potentially be medium or low impact.
- There are several places where the proposed standard could have unintended consequences with negative effects on reliability. For example, the requirement that all blackstart units registered as part of the regional reliability plan be classified as high-risk could lead to Entities reducing the number of declared black start units; an exemption based on an approved engineering study should be allowed.

- It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Functional Model or the Definition of Adequate Level of Reliability.
- This standard needs to be segmented into each applicable function and not try to use a "one size fits all" approach. If this path is taken, subject matter experts can help to better define what cyber systems should be in scope and out of scope on a very specific basis. This will eliminate much of the lack of clarity and misinterpretations of the present draft standard. It will also bring the focus back to protecting the highest risk elements with the highest level of protection and not try to do this for everything.
- Attachment 2 makes no allowance for system diversity and redundancy.
- The functions should be specifically covered in Attachment 1 under the impact categories they fit.
- Proposed attachment 2 looks comprehensive and well thought out.
- Replace "Functions Critical to the Reliable Operation" with "Functions that Affect the Reliability of the Operation". This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances.
- Please provide the basis for including each of the functions.
- There is concern with creating a definition and then supplementing the definition with an Attachment providing additional criteria and clarification of a term, as addressed with the High BES Impact comments. If a person were to just look in the NERC glossary then they would have no idea there were additional criteria defining a BES Cyber System. If an appendix or attachment is necessary, the definition should clearly reference the additional information.
- Clarify functions that are critical to reliable operation of interconnected BES, not isolated BES Subsystems.
- If you identify a control center in attachment 2 then this is not needed. Look at comment for clarity.
- Attachment 2 has potential for wider application and does not belong in a CIP standard.
- Failure or compromise of some cyber systems may not impact the operation of the subsystem for a significant length of time, allowing for repair. These systems should be excluded from the standard. For example, a PC based coal receiving unloading system. The fuel inventory on-site will supply the plant for a number of days, weeks or months depending upon the amount in inventory." No reliability improvement would be gained from applying cyber controls to this system.
- Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline

Specific Responses for Attachment #2

- Tools that are used in the planning horizon are not critical to BES reliability and should be removed from the proposed functions. (e.g. Unit Commitment under Balancing Load and Generation.)
- Consider combining 2, Balancing Load and Generation and 3, Controlling Frequency into one category.

- As a suggestion for consistency and to take advantage of the thoroughness of the info in the Concept Paper, why not use the nine functions identified in Figure 1 and Table 1 which include: 1) Contingency Reserve/Peakers; 2) Load Balancing, Frequency Response/Support; 3) Voltage Support/Reactive Power Supply; 4) Constraint Management; 5) Control and Operation; 6) Situation Awareness; 7) Restoration; 8) System Stability; 9) Load Management?
- We recommend reviewing for inclusion the following critical functions:
  1. Emission systems (with indirect impacts)
  2. Remote Cyber Support
- Recommend changing from "The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions." to "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES."
- Attachment 2 lists monitoring of spinning reserves which requires telemetry from every generating unit. This implies that every generating unit, regardless of size, falls under this standard. This would also seem to include each RTU and all the communication equipment back to the EMS. We have the same concern regarding calculation of ACE. This implies that all communication equipment back from the RTU for every input into the ACE equation.
- Definitions need to be clarified (e.g.):
  - "Governor Response" - is this movement of a governor to respond to frequency deviation?
  - "Providing Actual Reserves" - Are these systems that request additional generation in response to an event?
- 1. Dynamic Response – Disagrees with the inclusion of Spinning Reserve and Governor Response as neither of these is dependent upon a cyber system.
- 1. Dynamic Response – Spinning Reserve is listed which by itself is not an automatically triggered and not a Dynamic Response quantity. Units, or capacity so designated, is controlled by AGC. Governor Response should specifically mention AGC. Unless its control is addressable, Governor Frequency response should not be included as a part of the Cyber standard. Excitation Systems with Automatic Voltage Regulators are not listed and should be.
- 1. Dynamic Response – Under and Over Frequency Relay, Under and Over Voltage Relays are covered under Protection Systems. To call them out separately implies otherwise.
- 1. Dynamic Response - Generator governor controls may be purely mechanical or local electronic controls without connections to remotely accessible systems.
- 1. Dynamic Response – Is the bullet under number 1 that deals with under and over frequency relay protection intended for all entities that participate in under or over frequency load shedding or just the bigger entities as stated in Attachment 1 section 1.14? We feel that applicability needs to be clarified throughout the standard to ensure that it's interpreted correctly. If under or over frequency load shedding are considered critical to the

reliability of the BES, it should be clearly defined in the criteria for the impact categories of Attachment 1 what levels of load shedding fit each category like 1.14 of Attachment 1.

- 2. Balancing Load and Generation - This section should be clarified to address the balancing of electrical system load vs. electrical system "supply". It could be interpreted to apply to the pure generation unit control aspect.
- 2. Balancing Load and Generation – Disagrees that any of the listed activities is solely dependent upon a cyber system. These functions can be performed without employing a cyber system. The listed activities should only be included if they are solely dependent on computer systems, intranet or internet to allow access to multiple parties.
- 2. Balancing Load and Generation – Is "Manually Initiated Load shedding" the area of interest or the ability to identify. If "identify" this is under the scope of Situational Awareness in Item 8.
- 2. Balancing Load and Generation – These functions may be outside the Control Center. It is not clear if the intent would be to expand scope beyond the control center.
- 3. Restoration of BES – Disagrees with including this function, as most restoration plans assume the transmission operator's system has suffered a total blackout. It is extremely doubtful in this case that any cyber systems will be used, because each step of the process will have to be manually tracked. Inclusion should be determined on a case-by-case basis based upon the specific restoration plan.
- 4. Controlling Voltage – This Controlling Voltage section does not list "Transmit adjustments to individual units" (in response to a voltage schedule).
- 5. Managing Constraints – The drafting team should clarify item 5 "Managing Constraints" of Attachment 2. Could this include cyber assets used in the calculation of ATC? Tagging systems used to submit schedules?
- 5. Managing Constraints – Is the intent to pull systems such as Oasis and OATT into scope under managing constraints?
- 6. Control & Operation – Please clarify "control".
- 6. Control & Operation – Recommend adding parameterization, calibration.
- 6. Control & Operation – AGC should not be listed in the Controlling Frequency section as it is a Dynamic Response.
- 6. Control & Operation – The Control & Operation section needs to include Generator controls for AVR, and AGC.
- 6. Control & Operation – suggests the example should include "electronic" control rather than "all" control.
- 7. Restoration of BES – Cranking Path should be clearly defined for application in this Standard.
- 8. Situational Awareness – The Situational Awareness section is covered by the other sections and is not needed.
- 8. Situational Awareness - A definition or the intent of "Change management" should be included. Is this the management of change as cover in other sister standards?
- 8. Situational Awareness is too broad and needs to be better defined. In particular, the "change management" aspect of Situational Awareness is unclear.

- 8. Situational Awareness, bullet 5 – Frequency monitoring should be better defined so that the loss of a single monitoring point in a many point scheme is not a problem.
- 8 - Situational Awareness, suggest these words should be consistent with the real-time operations words for situational awareness in the Control Center definition. Recommend changing to: "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES."
- 8. Situational Awareness: It is unclear whether Change Management applies to IT Systems or change management as it relates to other work being performed on BES subsystems, for example repairs during a unit outage, or replacement of substation equipment.
- 8 – Situational Awareness. What is the team attempting to identify with Change management, and Current Day and Next Day planning? They both could be interpreted to mean outage scheduling applications.
- 9. Recommend changing 9- Inter-Entity Coordination and Communication from "The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES." to "only inter-utility data communications". Existing language would include voice communications.

Question 12: comments already discussed under other questions

- No additional comments offered by the SDT members

13. Comment Form Question # 13 Other Comments

13. Do you have any other comments to improve the draft standard?

Overview of Industry Responses

- Most Other Comments were already provided in response to earlier questions:

B. SDT Points of Agreement and Disagreement for Refining CIP-002-4

CSO 706 SDT Points of Agreement, Disagreement and Confusion in Terms of CIP 002-4

SDT Points of Agreement *regarding Industry Comments on CIP 002-4*	**SDT Points of Disagreement** *regarding Industry Comments on CIP 002-4*	**Industry Points of Confusion** *regarding CIP 002-4*
1. Flexibility is needed but may or may not be included in today's language	1. What is the CIP standard trying to protect against?	1. Do you start with R1 and work through R3 or is there more flexibility possible in CIP 002-4?
2. Functions of BES need to be considered, but may not be clear in today's standard language	2. Should it be connectivity vs. impact assessment	
3.Agree some form of inventory will be needed regardless of approach	3. We disagree on how extensive the inventory will be for each approach	
4. Any approach needs to result in a categorized list of cyber systems.		
5. We are addressing the range of cyber systems at play in the real time control and operation of the BES reliability	4. The Cyber system should inherit the category of the BES asset (indirect impact mapping) vs. basing it on an assessment of the external and internal threats (direct impact mapping)	
6. Bright lines will help to simplify the implementation and compliance with the standards	There should be flexibility and third party oversight.	
7. Where ever possible, the SDT should seek to combine steps and simplify the approach	5. Categorization should be based on threat/ reach/ connectivity	
8. We function in a compliance vs. a performance assurance framework.	If we are using a compliance framework we should stick with a CIP 003-009 structure.	
9. The standard should be designed so those implementing it know why they are protecting assets and systems.		
10.We are designing a compliance not a performance assurance framework"		

SDT Member Comments on Points of Agreement/Disagreement

- Is #8 a point of agreement or a desired outcome? We don't have a choice to ignore compliance.
- This is a point of agreement – to clarify, change to "we are designing a compliance not a performance assurance framework"
- Agree some form of inventory will be needed – disagree how extensive the inventory for each approach

- Are we not going to have third party oversight? Don't we have to have it to allow industry the flexibility they are requesting? Need that up there under points of agreement or disagreement
- #2 under disagreements should be deleted – redundant with #5
- Is it not best to stick with a 3-9 structure if we are using a compliance framework
- a disagreement - clarity in practice as to what a BES system is –
- #4 – change to inventory of BES cyber systems
- #1 and 4 – redundant? Get rid of #1 or #4? Strike #4
- #5 limits on scope or range of cyber systems? Yes
- #18 – revisit the severe VSLs? Change to "revisit the VSLs"
- #12 – need better definition – don't agree to remove it – okay can remove it if we cannot get a better definition – it is a task rather than agree/disagree
- #2 – overall flexibility or flexibility in approach? Flexibility in starting with R1 or R3

C. Review of Alternative Approaches to CIP 002-4

1. Categorization of BES Cyber Systems Based on Use of Routable Protocols

Dave Norton had circulated in advance of the meeting a proposal which suggested the categorization of BES cyber systems should be primarily based on use of routable protocols (threat/reach/connectivity?). The following proposal was presented for the Team's consideration:

Proposal: Categorizations of BES Cyber systems based on the potential impact of their compromise through the use of routable protocols as attack vectors.

- **Control center routable protocol = high**
- **Generation plant/transmission substation = medium**
- **All else = low**

SDT Member Comments before ranking the Proposal

- Categorization based solely on that, primarily on that, etc.?
- Categorization based on risk presented by external attack surface
- This is a test of whether categorization is based on routable protocols
- There is a baseline of things we have to do – some with more than others (medium/high)- routable protocols and intuitive obviousness
- Can live with doing an impact assessment with a second level based on connectivity – two level of assessments based on routable and non-routable
- Bright line is routable protocols – the attack surface – the impacts are variable
- Are we back to function?
- Concerned that equal focus on connectivity adds complications from a generation aspect – look at BES impact first and then connectivity

- Proposal is to scope it with primary focus on routable protocols
- How do we capture measurable criteria?
- Low is everything BES cyber – what makes it go to medium or high?
- Direct or indirect impact?
- Is this a complete substitute? Not a "primarily"? Yes
- Different definitions of "control centers"
- The three bullets are examples to illustrate the proposal

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	6	**4**	**9**	**2**	**1.5 of 4**

Comments after Ranking

- Clarification – were the bulleted items included? Yes. I don't agree with the examples
- But the examples tell me what it means.
- Can we test the current language for level of support? Or #2?
- The cyber system should inherit the category of the BES asset (indirect impact mapping)
- But this is a piece of R1 & 3 – this replaces only part of R1 and R3
- We tested the new proposal that came in after we tested the original proposal.
- We need to resolve this issue so we can move forward.
- #1 Ranking – flies in the face of what we have done up to this point of not looking at attack vectors until we addressed them in the controls
- #1 Ranking – basing the risk on the network – not a complete cyber security approach
- #2 Ranking because of the routable protocol emphasis – preferred broader view of original
- Need to make significant changes to current draft to address the comments from the industry
- Would move my #2 to a #3 if we removed the examples.
- Not an either/or decision – routable protocol may not be easy to define for many and serial is not protected from attack –
- Raises the technology up to the BES impact –
- It tells us where to put it in the controls and do not have to inventory all of your big iron – zero in on IP for more controls – two levels of rigor
- #2 Ranking – routable protocol and attack surface may be a red herring – agree with concept but need an alternative – talking about a security of connectivity – intent is connectivity but routable protocols will not get us there
- We need a categorization method to start with – then work on the controls – a categorization method we can put controls onto
- Need a modifier – the inheritance as a base with connectivity (or lack of) as a modifier to bring it off of high.
- Don't see how you can let go of the BES asset.

2. Jay Cribb Proposal- Combining Cyber System Impact on BES with Connectivity

Jay Cribb presented his proposal in which he tried to combine both the cyber system impact on BES and connectivity as shown below.

Cyber System Impact on BES →	high	medium	low
Connectivity ↓			
Routable	high		
Non-Routable	high		
Stand Alone	medium		

The SDT ranked this proposal as follows:

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	4	**13**	**3**	**0**	**3.05 of 4**

- Looking for clarifications in a sloppy system
- The SDT needs to be on board with basic concepts – we are shoehorning everything into h/m/l – may need to reconsider
- Looking at concepts at different levels and trying to merge them together.
- Are these the only criteria?
- We should remove the e.g.
- I voted on this as a model not as criteria.
- Need to review more of the Industry responses – not sure we can ever be clear as to what is medium.
- Not looking at h/m/l requirements – these are impact levels.
- FERC asked us to look at it – and it doesn't work.
- I think it does work – still works if we do not have a moderate level and we only have a high/low assessment

- Chair John Lim asked Jay Cribb, Scott Rosenberger and Dave Norton to discuss this proposal in the evening over beer and invited other members to join and bring back a revised proposal based on Tuesday's discussion.

3. Revised Hybrid Approach

Stu Langton reviewed with the Team where we are, the request to a group to work on and bring back a proposal to the full group this morning, the difficult nature and complexity of the task at hand – we will continue to have disagreements but have met our previous deadlines and will continue to work to meet the upcoming deadlines – remind members that consensus doesn't mean we have to all agree and that we cannot disagree sometime – differences are okay – if

75% want to move on, then we will – we need the minority to hang in there and keep working with us.

Scott Rosenberg presented the revised proposal and spoke about risks presented by connectivity and the challenges in defining terms accurately. The BES impact will still be h/m/l, but the proposal introduces the connectivity risk of routable versus non-routable. The matrix similar to one used before. May look like a high, high-medium, medium, medium-low and low. They were trying to avoid incredibly detailed inventories. You would like to be able to split a system into high or medium, slice and dice as needed to limit having to treat everything high – down to bus or breaker level. If we do our perimeters right, we can limit the columns for audits. We need a formula or guidelines the auditors can work with. This proposal reconciles the good work done so far on BES side and on the cyber side. Looking to see if the SDT thinks this process is agreeable and then would look at analysis.

SDT Comments

- Absent an inventory how can you say you identified everything that needs a control and if the control is adequate?
- Maybe we need to identify capacity as the starting point.
- Need to avoid mis-categorizing or not capturing
- Not taking away categorization process we already developed but we do need to refine – comments to indicate the process is not clear – on top of that, if you identify the right assets, then you prioritize and refine categorization based on connectivity. If we do it right we will protect the right assets and not over protect the wrong assets. Join the approaches together but recognize this need more refinement to clarify issues.
- BES requirement was seen as site specific – follow up with cyber system inventory and then based on connectivity determine its impact.
- This attempts to allow you to justify not having to put too much protection on assets that are not interconnected.
- Once you figure out what is protected, you then look to develop protection controls.
- Sounds like current 002 for establishing the inventory with a new layer of prioritization.
- Need to nail this down so the small groups work from the same framework.
- Connectivity? Three categories: connected to routable network (clearly in), relay with Ethernet and substation network but no wire connecting it to the switch capable of being routable (in or out?) Need to discuss further what connectivity means. Third – not connected at any point.
- Now have direct mapping of BES assets to cyber systems
- System idea – matrix for categorizing your cyber systems
- Something connected serially to a routable box? That would be connected
- If I plug my pc in through another serial connection is it connected? Maybe not.
- Is it assets or system based? Categorize the BES asset systems – think in terms of running systems through a litmus test. Can you control it or not.
- Concern is about hitting multiple sites in order to impact the grid.

- Some divergence in the sub group on this issue – control systems versus ability to control a system – needs further refinement and discussion.
- Whether rout-ability or controls needs discussion once we agree to go with proposed connectivity approach – lets not get hung up on the criteria at this point.
- Where do we spend our money to protect the system.
- How did you determine what is scoped into a system? Assessing impact level of BES asset based on its connectivity – how do you determine its level of connectivity if it has multiple connectivity methods?
- Do we need to skinny down attachment 2?
- Problem with "system" – what do you call a system? Where do you draw the boundary? Need to define better, then connectivity between sites establishes the level.
- Type of connectivity matters – category of controls you apply depends on the type of connectivity.
- Need to better define system in CIP 002 so we know we can break it up as needed.
- The details we will have work through together as a team.
- Definition in form 417 – any need to consider as part of teamwork?
- Need to see both proposals to get the full picture (second proposal from Phil to combine R1 & 2)
- Still need to address controls, what is relevant to real time control – and need to address complex issue of "connectivity"

"Include connectivity as a factor in the BES Cyber System categorization"
Revised Proposal: Matrix for Levels of Controls to Be Applied

BES (attachment #1 of CIP 002-4)	High	Med.	Low
Connectivity-Routable/Dial-up	High	High	Med.
Non-Routable	Med.	Low	Low
Not Connected	Low	Low	Low

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	12	**4**	**2**	**0**	**3.6 of 4**

Comments After Ranking

- 2 = I do not see the difference with what we put out to the industry –
- It is modified by connectivity
- 2= don't like doing the BES asset assessment first
- still need to figure out what functions are in the attachment – scope it out some more
- must address Bulk power as the first step for industry support and this let's us do that
- small group will meet this evening to review and fill in the concept with text to help clarify concept – John Lim, Phil Huff, Rich Kinas, Jay Cribb – others can join them

4. Proposals for Combining Attachment #1 and #2

Phil Huff offered the following successive proposals for testing acceptability related to combining Attachment #1 & #2 for the SDT to rank. The SDT reviewed and ranked three versions of the proposal. Before ranking members discussed the proposal:

SDT Comments on the Proposal for Combining Attachment # 1 & #2

- Direct impact on BES cyber system – what does that system do?
- Where do we draw the lines in the BES cyber system?
- Other criteria that may need to be considered – may need to modify.
- What if system only meets or controls part of the aggregate number?
- Need a comparable format for both proposals.
- Attachment 2 goes away and section A is changed to say cyber systems
- Connectivity is mentioned over 80 times in the comments – controls over 40 times – important concepts we need to address.
- By dropping the last half of section B, we would clarify and provide a bright line for compliance/
- For Medium/Low Criteria: Cyber systems controlling/monitoring/alerting/protecting a Generation Subsystem with aggregate rated name-plate generation of x000MVA or more. (drop rest of section?)
- Do we need to line up with higher numbers used by NERC?
- We assume there is a size and impact relationship – but that is not clear – VRFs are the mechanism for connecting.
- Multiple small risks can add up to a large risk – need to get back to and discuss the relationship.
- Concerned about dropping Attachment 2 – without the functions are we opening ourselves back up to including systems that do not control BES?
- Clarify BES cyber system and cyber system functions
- Develop the modification methodology for the categorization of BES cyber systems

a. 1st Version Proposed by Phil Huff

Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed (the Criteria is the Span of Control).

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	2	**9**	**9**	**0**	**2.65 of 4**

SDT Comments after Ranking

- Cyber system inherits categorization of attachment 1 – concern is for the tie to attachment 1 rather than connectivity
- Categorization is based on what the system does
- Like the concept of merging 1 and 2 but needs to be criteria of BES system – cyber system needs to be a subsystem – remove “cyber” and remove last parenthetical for me to support
- Not sure what the parenthetical meant

- Huge effort to map the span of control back to the substation gear – we tried to map functions back to bright lines and it was too complicated
- I like idea of combining, but the criteria may be a problem
- There is a way to address criteria noted in comments from EPSA
- Too complex.
- This might be a way of reintroducing the serial exemption.
- Too many permutations.
- Is it possible to move forward without resolving this issue?
- Attachment 2 is complex in itself –
- Is it the fact there are criteria or is it what the criteria are? The latter we can work on together – if the former then we have a fundamental question.
- Comments said we need criteria – general agreement in industry that we need criteria – but not on what the criteria should be.
- Span of control concept seems to be the source of most concern here.
- Can we turn to others to establish the criteria?
- We had agreement that the type of communication needed to be included.
- Informal survey question to the industry? Given we want a bright line, what criteria should we use to set the bright line?
- Can we extend beyond our industry?
- How would survey question differ from Question 8 we already asked? Look to those comments for guidance and suggestions.

b. 2nd Version Proposed by Phil Huff

Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed. ~~(the Criteria is the Span of Control).~~

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	1	**11**	**6**	**1**	**2.4 of 4**

Comments after Ranking

- We need to understand what we are going to do with the attachments to move forward – cannot write requirements without the attachments.

c. Revised Concept of Combining Attachment #1 #2.

On Friday morning, Dave Revill presented concept of combining Attachment 1 & 2 that was discussed overnight by a group including John Lim, Phil Huff, Dave Revill, Rich Kinas, Patrick Leon, Joe Deotzel and Dave Norton. He noted that under the proposal:

- Attachment 2 becomes more of a guidance document
- Res shall categorize its BES cyber systems by applying criteria in CIP 002 Attachment 1
- Changed ~~BES Subsystems~~ to <u>BES Cyber Systems</u>

- Changed Generation ~~Subsystem~~ in Attachment 1 to Generation facility.
- Move attachment 2 to a guidance document to identifying what immediate effect on real-time operations means

This proposal combines Attachment 1 and Attachment 2 by tying the criteria in Attachment 1 to BES Cyber Systems that immediately (i.e. 15 minutes or less) affect real-time operation. Attachment 2 is moved to a guidance document for identifying Cyber Systems that immediately affect real-time operations. (including the connectivity matrix)

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	8	**10**	**1**	**0**	**3.4 of 4**

Comments after Ranking

- Don't believe connectivity should be at the categorization level but should be at the controls level,
- 2= could vote a 3, but the "how" has a problem
- John L., Dave R, Rich K. and Jackie C will continue to work on the revisions to 002-4 and will pull themselves off of the control sub-teams to work on this in the short term.

R1. As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize its BES ~~Subsystems~~ Cyber Systems ~~under its ownership~~ by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES* ~~Subsystems.~~ *Cyber Systems*. (*Violation Risk Factor: High*)

Attachment 1: Criteria for BES Impact Categorization of BES Cyber System
Cyber Systems that would immediately effect real-time operations for:

- Generation ~~subsystem facilities~~ with aggregate rated name-plate generation of 2,000 MVA or more.
- Etc.

Move Attachment 2 to a guidance document to identifying what *Immediate effect on realtime operations* means.

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	15	**6**	**1**	**0**	**3.6 of 4**

SDT Discussion of the Proposal

- Doesn't matter where facility is if it is doing real time operations.
- Not vastly different than what we do today – big pro of this is that some of the vague terms like BES subsystem are gone – looking at cyber systems with real time impact.

- Now coming up with categorization based on some rating of facilities (a defined NERC term).
- Not changing anything in Attachment #1 except subsystem to facility – same criteria – still have to produce all generation, transmission, control center information for the auditor.
- R1 provides bright lines of generation of X name-plate rating – smaller entities do not have to jump through all the hoops.
- Do we trust entities to identify all the functions that impact real time operations?
- Problem with "facility" – introduces a new challenge for defining it – not just what is inside the fence.
- "facility" is not capitalized (i.e. in the NERC glossary) which is dangerous –
- It should be capitalized to be a defined term – but that presents new issues given the definition – it does not sound like a plant or substation – also nuclear industry has different definition that includes inside the fence.
- Can we say "generation facility or combination of facilities?"
- A BES cyber system that can affect more than 2000 of generation – strike the term "facility"
- Levels of categorization? What are the systems that will go into the list?
- This is meant as one example for high – others need to be included for generation, transmission, etc.
- What is the method for coming up with other criteria?
- Focused on the proposed concept – criteria the same as today
- "Real time"? Operating horizon criteria? It is a term defined in NERC glossary? We will need more detail.
- If use Attachment #1 how do we come up with things in main category if looking at cyber systems first? How do we know it impacts a high generation thing if we do not already identify high generation thing first?
- Doesn't really matter if we understand what generation is and what transmission is – how much of the generation is impacted – gets you off the hook for documenting all generation and making it subject to an audit.
- Careful to use accurate terms – have to identify a complete list of BES cyber systems and then determine high and medium base on criteria to be developed.
- Real time is a time horizon – "done within one hour"
- Like that it focuses on real time and brings in connectivity – may still need to tweak Attachment #1 language regarding cyber systems into h/m/l
- "Immediate"? Included to respond to industry comments,
- This concept removed ambiguous terms and provides a bottom – does not include everything in North America with a chip in it.
- Connectivity is implied somewhere?
- It would be in the table or matrix developed yesterday
- Connectivity could be left as an aspect of the controls – this does not start off with a huge inventory list which is a good thing.
- Not directly connected, but are collaterally connected to devices that are connected directly – how do we handle those?

- Where does a system that maintains targets on relays that can modify settings come in?
- These are real-time questions that we need to account for.
- Worried industry will not understand where the bright lines are with this concept.
- We may be cutting off options too soon – like to see us work with this and other options as sounding boards.
- Have to have a starting point for auditors can start with – 69 KRB might work.

D. Small Group Review of CIP-002-4 Industry Comments

The SDT reviewed group preferences for working in small groups to address the industry responses to CIP-002-4. The small groups agreed to meet together starting Wednesday morning to draft potential changes to draft 002-4 in addressing comments based on plenary discussion today and draft possible responses to comments then review suggested changes with the full team during the afternoon. It was agreed the SDT needed more work on the points of disagreement as guidance to the small groups looking at 003-009 controls. Group B and D need a better understanding of Questions #5 and #2/3 in order to do their job.

- **Group A- Definitions, Purpose and Other Comments** (Questions 1, 2) Review industry comments (overview) and agree/disagree/confusion items: Frank Kim(1), Jeff Hoffman(1), Scott Rosenberger(1), Sharon Edwards(1)
- **Group B Attachment 1- Criteria for Categorizing BES Cyber Systems** (Question #3,4,8 & 12) Review industry comments (overview) and agree/disagree/confusion items: Doug Johnson(1), John Varnell (1), John Lim (1) Jim Brenton
- **Group C VRFs, VSLs** (Question #7) **and Measures.** Review industry comments (overview) and agree/disagree/confusion items: Joe Doetzl, Phil Huff, Dave Revill, Dave Norton
- **Group D Standard Requirements** (Question #6) **(R1-3)** Review industry comments (overview) and agree/disagree/confusion items: Gerry Freese(1), Patricio Leon, Jay Crib (1), Jon Stanford (1), Bill Winters (1), Rich Kinas(1)
- **Group E External Oversight** (Question #8) Review industry comments (overview) and agree/disagree/confusion items: Keith Stouffer (2), Kevin Sherlin (2)

Bob Jones reviewed the breakout groups noting that each team should have a group report and that question 8 would go to Group E (Kevin and Keith). Each group would look at industry comments and the Team's discussion to draft potential changes in CIP 002-4 (for full team consideration later this afternoon).

SDT Comments on the CIP-002-4 Small Group Charges

- Not sure how we incorporate the models we just expressed support for?
- Can't write criteria at this point – Group C, once done may need to divide up among other groups
- What should group B try to address?
- Question 8 is under B and E? Should question 4 be assigned to E? Assign Group E to look over comments in Questions 1, 4 and 8

- May need to reorganize the groups and topics – Group C cannot address VRFs without clearer direction on criteria.
- Group C could develop a potential concept for how to develop VRFs based on review of the industry comments.
- Group B should look at comments on actual values and structure from the industry.
- Group D should draft or change requirements we have reviewed based on the SDT comments.
- Group A will need to struggle with possible definition of BES cyber system.
- Are we being asked to draft general responses? Assignment is not to draft summary response yet – take notes for later – assignment now is to refine CIP 002-4
- Bring back suggestions for changes to 002-4 – don't get too bogged down in refining the language or resolving all issues/questions

Small group sessions took place during the early afternoon followed by a plenary reports and reviews of their work.

1. **Group A: Definitions Report**

- Incorporate definitions into the attachment #1
- Intent to move them in as a descriptor
- Cascading is a glossary term
- Cyber system and BES cyber system combine into one definition
- with note that this is determined by the criteria in attachment #1
- do we need to scale it down to control systems? We may need to formally define control system rather than just describe it – may be very difficult to come to agreement on definition
- Can you clarify the note?
- Non-critical cyber assets inside an ESP – work in progress
- BES subsystem definition revised with separate definitions for generation, transmission and control center definitions (To be determined)
- Generation – can we reference the ad hoc NERC groups work last fall?
- May not want to reference, not exactly on point and has not yet been approved
- SAR just opened and group not yet appointed
- Need to loop in the requirement for interconnections – generation/owner question
- Add facilities needed to connect the generation to the transmission system
- Control center in control of multiple generation sites – combined units because they share the control system? May be covered by control center definition
- In effort to be consistent use generator facilities ratings, not the output
- Do we need to define generator subsystem? Is it covered by cyber system definition?

- If aggregate based on control center then each site takes on the level of the control center?
- The key is the risk
- Did not finish the control center definition – do question whether substations should be included
- Would take a few more hours to finish

2. Group B: Attachment #1 Report

- Question 8
- Reviewed action items
- Drop back to two tiers – leave open until controls work complete
- Use the nameplate or rating to prevent gaming
- Criterion should be separated into two with one for Protection System for which the voltage distinctions would apply and second for SPS and RAS for which the voltage distinction has no meaning.
- Change language to all control centers to get around issue of only Bas and TOPs required to have backup control centers
- Add requirement for engineering assessment approval
- Special protection systems – careful how we use it given the glossary definition and what it includes – may include more than we intend
- Engineering assessment – key is who gets to validate the assessment and does the model cover cyber systems – can't write your own rules to get the results you are seeking
- May be unintended consequences from alternative of just having bright lines
- Inner workings of cyber system placed on top of the generation system – expertise available in each but not necessarily both – the key in the assessment is what is the problem statement and who creates that statement
- Requiring all control centers to have backup control centers? No, simply need to clarify the language

3. **Group C: VSLs Report**

- Determined the percentage approach would be the best – current CIP version is binary, miss one and it is severe –
- Premature to develop VSLs until you determine the requirements

4. Group D: Standards Requirements Report

- Need to know impact of CIP 003-009 – added to schedule
- Need for an engineering analysisi and a regional authority should approve it
- A regional authority should approve eng. Analysis
- Change? Impact to the categorization

- Engineering analysis shall cover by CIPs information protection requirements
- There is no need for a master list of all BES subsystems. However BES subsystems definitions is required

SDT Comments and Questions?

- Who is the regional authority? What about region to region?
- RE will be responsible to comply with requirements – owns and operates will be toned down, know they have a protocol but not what cyber systems cover
- Where there are owner/operator relationships, need to work out responsibility and capture in their contracts
- The person that is operating the equipment understands capabilities and should have responsibility
- Becomes a compliance liability issue and who has to pay the fine – cannot avoid – assign to someone – may need to look to other standards for examples of how the issue is handled
- Currently compliance varies – there is not one way to do it
- Can flow down requirements to help meet responsibility but can't pass on the responsibility
- This is a legal problem for others to determine

5. Group E, External Oversight- Report

- Oversight is problematic (varied approaches and issues offered in the industry comments) – no
- RC needs to be involved in establishing the criteria for the engineering analysis or approving the assessments
- Engineering assessment is married to liability and needs to be resolved
- A 2 category approach may lessen the need for engineering analysis
- Clear bright lines for each region may lessen the need for engineering analysis
- Engineering analysis may be used to develop the bright lines

E. CIP-002-4 Next Steps

On Friday morning the SDT discussed next steps regarding refinements to CIP-002-4 and the development of a response document for the industry's consideration. The Chair proposed and the members agreed that a team of 4-6 members would be formed to work on refining 002-4 between now and the March meeting in Phoenix where they would present a new draft back to full team as well as a response document. The team may also continue after March.

SDT Comments on the Proposed Next Steps

- Are we setting sail without a rudder?
- Review two items of consensus – review of concept and the connectivity as a factor (and the combining attachment 1 & 2 without the parenthetical.

- Can we flesh out the concept model?
- Does concept model include the merging of the attachments 1 & 2?
- This also melded the communication concept into the model
- Concerned we did not fully address the concerns – feel we still have two models without fully understanding how they are melded together – danger of differing interpretations.
- May need to flesh out Jay's concept with phrases and words?
- Can we take a few of the criteria in attachment 1 and test them? Put requirement on paper.
- How you arrive at the h/m/l BES cyber system impact in terms of criteria is the key.
- Confusion on how h/m/l is used in Jay's concept versus the original proposal outlined by Scott Rosenberger. They seem different.
- Alternate ideas may offer more clarity – review as plus and minuses.
- Current attachment #1 is the top row of the original concept offered by Scott Rosenberger – an inherited model- title with "level of controls to be applied" – this is a site/facility concept.

III. CIP-003-009 SECURITY CONTROLS REQUIREMENTS

A. Security Controls Requirements Sub-teams Progress Reports

Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson(Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin

The report was delivered by Doug Johnson who noted they have reviewed 006 and 004 and that they need to coordinate with the electronic access groups going forward. He reported they did get through the DHS items.

Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*

Scott Rosenberger reported on the Subteam's progress noting he had met with Jeri Domingo Brewer to review the efforts in Tucker and the Subteam had difficulty meeting as a team since the January meeting. They have however completed an initial shot at h/m/l and will be working forward.

Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*

Sharon Edwards reported on the Sub-team's work. They had one interim meeting together then each member has worked on assignments which are almost complete. They met one night meeting in Austin and plan another in a week before combining into one document. They have developed a collaborative site to review documents.

SDT Questions

- Is there a format we should be using? Jay's or Rob's A. document from Tucker meeting? Want to combine the 25 separate documents they have into a common format other teams are using
- Rob's was a summary document
- Spreadsheet did not work for John Varnell's group – they put in to a different format – can't put text into Rob's spreadsheet document

Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Dave Revill, Phil Huff (Lead) *Observer Participants: John Fridye*

Dave Revill provided the report noting they don't have a collaborative site to share documents but they are mapping controls to the existing CIP requirements and analyzing the difference between CIP and other standards.

Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton

No report was given for this subteam.

Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell

Jay Cribb reported on this group's effort including one meeting where they reviewed portions of CIP 005& 007 and reviewed corresponding DHS and other catalogue of controls. Finally they developed four high level questions for additional guidance to all the groups

B. Guidance Questions for the Security Controls Requirements Sub-teams

Following the Tucker meeting, the Drafting Principles were revised by Phil Huff based on team discussion and sent back around to team members. Phil reviewed the steps in the team process and proposed deliverables (separate document) for the sub team work on the proposed control requirements, 003-009, with impact and environment applicability

Jay Cribb introduced and reviewed the four questions the Operations Security group had developed noting, in essence, the NERC CMEP and ROP have the SDT in a very constrained

box currently. We've got a CIP-002 structure that is on a path that won't fit in that box. He suggested we need some determinations on these things before we get too far down the road and hit a roadblock.

1) **How we are going to handle writing requirements that apply to 'BES Cyber Systems' rather than 'Critical Cyber Assets'?**
   The object to which requirements are applied has changed rather drastically and we need to determine how an entity takes a requirement applied to a 'cyber system' and knows what to do to what components of that system in a clear, repeatable, auditor-must-come-to-the-same-conclusion kind of way.

SDT Discussion Points

- Access control – we each have different systems that join into one organism – components of the whole.
- How do you apply virus protection to one component and not to another connected component? How do you write requirement to apply to operating systems that can be compromised without bringing in other components?
- Don't need protection on every relay or printer – may need to do a better job of writing the requirements in the future.
- Authorizing access to a cyber system? If so, is that access to every component? Authorized access to a system may not include physical access.
- Do we need to stratify for new and old systems? The latter were not designed for the current cyber system.
- How much of the details are in the guidance? Is there something between requirements and guidance? Such as specifics on password protection.
- May need to get more granular than just h/m/l to fit in the wide variety of circumstances – a risk management system.
- Have to get more granular, more prescriptive in tables – any guidance will be treated as required in practice – otherwise may need an engineering study to say why you did not follow guidance to avoid liability – may not be able to answer this question
- TFEs – address in question three.
- Talked about using tables to outline the specifics.
- Access control – the extent or reach of the controls can become expensive and time consuming as we move out to remote sites.
- At least three or four levels of access you can make work – but be clear how far the access goes.
- Controls need to be applied to the system.
- We want to go to "specific" rather than "prescriptive" – the latter is telling you how to do that – need to be specific to be clear for audits.
- Are there other documents or bodies we can reference or build on for our use?
- Moving forward apply at a high level and note where specificity may be needed
- Compliance is more difficult in virtual world where harder to separate pieces – not dealing with physical items as much as before

- How we chose to use words and what words we chose to use will matter to allow clarity for audits – struggle to write appropriate requirements and measures.
- Many different compliance methodologies for the same requirement – auditors recognize different solutions across the industry.
- We use language differently – legalese, cyberese, etc.
- Make sure requirements and measures can stand the test of time.
- Most standards are not working to a prescriptive measure.
- Helpful to know if standards development allows for more flexibility.
- Referring to other documents and tying them to the requirement will not work because those other documents could be changed outside or independently of our process – can go into guidance but not the requirements
- Want to change the NERC process for setting standards measures – why continue with a broken system.
- We can use examples as part of the guidance.
- What is our direction as a team as to the guidance and measures? How do we go about developing engineering based measures in our standards? We need a body that can certify approaches? We need to get to measurability and we do not have way to certify measures
- Staff will go back to NERC to try and figure out how we can justify the thresholds or measures we use in the standards
- Putting in bright lines in 002 but removing some of the brightness in 003-009 – currently have bright yes/no requirements but moving toward more flexibility in how we meet measures
- Can clarify the what but not the how – the how is a compliance issue

2) **At what level are we to write the requirements?**
We have some that are taking the DHS controls and tweaking based on CIP. We have some taking the CIP requirements and tweaking based on the DHS controls. But the two are written at vastly different levels. Which is it? Should we:
    - Take the DHS controls and tweak them based on CIP; or
    - Take the CIP requirements and tweak them based on the DHS controls

SDT Discussion Points
- Right at the correct level – may be the best answer to the previous questions
- Have to get to a higher level or end up writing 100 pages for every contingency in each requirement
- Requirements should apply to either 1. The BES cyber System as a whole or 2) components of the BES Cyber System. When a requirement only applies to specific types of components, describe those types of components to determine where component classes exist. Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System
- Just meant to guide sub teams in writing requirements for review at the next meeting – drafting guidance –

- Answer to second from discussion of the first may by be the second bullet to take the CIP requirements as the base
- Taking CIP language to a higher level, changes the words and may be harder to measure
- Not all of the subject areas need the same level or amount of change – also may not be a one size fits all – some may be approached better from CIP and some from DHS
- Utilize the words that are there, change the ones we need to and start with either CIP or DHS as appropriate
- Careful about unintended consequences – everyone understood TFEs but ended up with unintended consequence
- Any base of information coming back from audit spot checks that highlights issues we need to incorporate into our rewrite?
- Can we request a summary from the regional auditors working group?
- Be sure we are not just taking one view point or opinion
- CCWG is such a regional group that would give a broader view than just a few individuals – trends, problems and issues they would like for us to be aware of as we move forward
- Asking for information on what difficulties they face, not asking for their direction

3) We've got to have some kind of ruling on the topic of compensating controls in a NERC CMEP world.

- Are we writing requirements at a detailed level with very discrete measurement and where compensating controls are not allowed (or just simply known as TFE's)? If so, are we going to add "where technically feasible" language like the current NERC ROP requires us to do on every requirement so that TFE's can even be requested?

  or

- Are we stating a control objective and how the entity meets it is up to them?

SDT Discussion Points

- Addressed in part above
- We may only be able to carefully craft the words of the requirements because that is what you will be held accountable for in an audit
- Compensating controls – NERC did not take it off the table but suggested need careful oversight methods for accountability
- May need to educate FERC that there are no guarantees in cyber protection – they want yes or write us a check –
- Definition of "within"? How do we comply if we are not sure what it means?
- This is not a SDT issue to resolve – careful how we write requirements – have to leave at level of implement a boundary protection, but not the how to do it

4) We need a standard way to not only handle the difference in impact and environment (CC/Gen/Tran), but the difference in cyber system/device class.

Control Centers, Plants, and Substations all can have Windows based HMI's for example. But plants typically have PLC's, and substations have IEDs. We need a standard way to handle the device classes so that we don't write requirements for the "IT style" cyber assets

that end up generating TFE's for every other device class.

- How should we handle the difference in impact and environment (CC/Gen/Tran)?
- How should we hand the different in cyber system/device class?

SDT Discussion Points

- Some overlap with earlier discuss
- Have to write controls to apply to the class of device
- What are the standard device classes and definition of each?
- Better off avoiding too high a level of control
- Difference in environment? Cost benefit analysis troubles me as a tool due to variables between entities and environments
- Need more than a cafeteria approach of what looks good or appealing

C. Additional Sub-Team Drafting Guidance Statements

Based on the SDT discussion the following guidance statements were proposed to be added to those developed at the Tucker meeting:

Underlined Added Guidance from February 19 SDT Discussion

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

1. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
2. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
3. **Specific not prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
4. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
5. **Develop the requirement language** for each security control identified in step 1.

a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog.*

6. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
7. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
8. **Address specific directives from FERC Order 706** that may be applicable to the requirement.

9. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, ~~on the basis of~~ consider the cost ~~vs.~~ in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
10. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
11. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.
    (c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.
12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.

IV. NEXT STEPS

The Chair reviewed the progress made at the meeting and the need for the sub-teams to continue to meet between Austin and the Phoenix meeting to bring draft language for the security controls for review by the full team. He also noted the agreement on a revised schedule and the formation of a Team to take the CIP-002-4 draft and make refinements and develop a response document to the industry comments.

The Vice Chair agreed to work with the facilitators to revise the Sub-team drafting guidance statements based on this discussion and circulate them in advance of the March meeting.

The meeting adjourned at 12:15 p.m.

_____

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 19th Meeting Agenda
February 16, 2010, Tuesday- 1 PM to 5 PM CST
February 17, 2010 Wednesday- 8 AM to 5 PM CST
February 18, 2010 Thursday- 8 AM to 5 PM CST
February 19, 2010 Friday- 8 AM to 2 PM CST
ERCOT Austin MET Center
7620 Metro Center Dr.
Austin, Texas 78744

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

Proposed Meeting Objectives/Outcomes

- Review the CSO 706 SDT 2010 Work plan
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan
- Review, discuss industry comments and identify issues raised to be addressed in refinements;
- Review, refine and adopt a revised CIP 002-4 for posting
- Receive progress reports and review assignments for Security Control Sub-Teams
- Agree on next steps and assignments

Draft Agenda

Tuesday	**February 16, 2009**
1:00 p.m.	Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of January 19-22, 2010 Tucker SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review of CSO 706 SDT Workplan- February-December, 2010- *Stu Langton*
1:20	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:30	Update on CIP Communication Plan, including Webinar Report
1:45	Review of needed CIP-002-4 Documents for posting: Introduction, Comment Form, Requirements, Attachments, Implementation Plan.
2:00	Overview of the Industry Comments on the CIP-002-4 *John Lim and Phil Huff*
2:45	*Break*
3:00	Identification of Key CIP 002-4 Issues Raised by Industry Responses to Comment form Questions (1-13)
4:30	Review and Initial Discussion of Other Proposed Approaches to CIP-002-4 *(Dave Norton etc.)*

5:25	Review of Proposal for Wednesday's Agenda
5:30	*Recess*

Wednesday	**February 17, 2010**
8:00	Welcome and Agenda Review- *John Lim & Phil Huff*
8:10	Discussion and Consensus Testing of Concepts and Responses to Industry Comments and Critiques
10:15	Break
10:30	Discussion and Consensus Testing of Concepts and Responses to Industry Comments and Critiques
12:00	*Working Lunch*
12:45	Review and Agree on How to Refine CIP 002-4 *(Full Group or Drafting Sub-Groups)*
1:15	Clarify Issues and Begin Draft Possible CIP 002-4 Refinements *(Full Group or Drafting Sub-Groups)*
4:00	If Sub Team Formed- Initial Reports and Flagging Issues Needing Full Team Guidance
4:55	Review Assignments and Thursday Agenda
5:30	*Recess*

Thursday	**February 21, 2010**
8:00	Welcome and Agenda Review- *John Lim & Phil Huff*
8:05	Approve Tucker Meeting Summary Approve Revised CSO 706 SDT Schedule
8:15	Review Proposal from Last Night's Categorization Alternatives Discussion (*Beer Brigade)Scott Rosenberger (Jon Stanford, Frank Kim, John Lim, Dave Norton Brian Newell)* Review Proposal for Combining Attachment 1 and 2 *Phill Huff*
10:00	Convene Drafting Groups to Complete CIP-002-4 Refinements
12:00	*Working Lunch*
3:15	Break
3:30	Drafting Group Reports and Full Team Consideration and Consensus Testing
5:15	Review CIP 002-4 Assignments and Friday Agenda
5:30	*Recess*

Friday	**February 22, 2010**
8:00	Welcome and Agenda Review- *John Lim & Phil Huff*
8:05	Review and Agreement on CIP 002-4 Proposal from Last Night's Drafting Group- Formation of a CIP 002-4 Drafting Team and Next Steps
9:15	Communications Plan- Gerry Adamski
9:30	Brief Security Controls Requirements Subteam Progress Reports Review of Drafting Principles and Guidance (from Tucker meeting) Review of Key Questions Security Controls 003-009- Operations Security Sub-Team and suggestions for refinements of the Principles and Guidance document
10:00	*Break*
10:15	Continue Review of Key Questions and Answers

12:00	Review and Agree on Next Steps for Developing Security Controls (CIP 003-009) and Work plan for March 2010 Meeting on Security Controls and CIP 002-4 Review Meeting Evaluation
12:15	*Adjourn*

Appendix # 2 Attendees List
February 16-19, 2010, Austin, Texas

Attending in Person — SDT Members and Staff

1. Jim Brenton (Wed-Fri.)	ERCOT
2. Jay S. Cribb	Information Security Analyst, Southern Company Services
3. Joe Doetzl (Wed)	Manager, Information Security, Kansas City Pwr. & Light Co.
4. Sharon Edwards	Duke Energy
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Frank Kim	Ontario Hydro
10. Rich Kinas	Orlando Utilities Commission (Wed.)
11. Patricio Leon	Southern California Edison
12. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY
13. David Norton	Entergy
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy
16. Kevin Sherlin	Sacramento Municipal Utility District (Wed. Thurs.)
17. Jonathan Stanford	Bonneville Power Administration
18.Keith Stouffer	National Institute of Standards & Technology
19. John D. Varnell	Technology Director, Tenaska Power Services Co. (Wed. Thurs)
20. William Winters	Arizona Public Service, Inc.
Roger Lampilla	NERC
Scott Mix	NERC
Howard Gugel	NERC
Gerry Adamski (Fri by phone)	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

21. Rob Antonishen	Ontario Power Generation (Thurs)
22. Jackie Collett	Manitoba Hydro (Wed/Thurs)

Others Attending in Person

Jason Marshall	Midwest ISO

Others Attending via WebEx and Phone

Stacy	Bresler	sbresler@wecc.biz
Chuck	Coulter	ccoulter@wecc.biz
Bryn	Wilson	wilsonwb@oge.com
Rod	Hardiman	rchardim@southernco.com
Annette	Johnston	ajjohnston@midamerican.com
Bryn	Wilson	wilsonwb@oge.com
Jerome	Farquharson	jfarquharson@burnsmcd.com
Bill	Glynn	bill.glynn@westarenergy.com
Bill	Keagle	william.a.keagle.jr@constellation.com
Keith	Walters	step@eei.org
Joshua	Axelrod	jmaxelrod@gmail.com
Steve	Newman	srnewman@midamerican.com
Justin	Kelly	Justin.Kelly@ferc.gov
Don	Schopp	donald.schopp@constellation.com
Bryn	Wilson	wilsonwb@oge.com
Jack	Vranish	jack.vranish@pacificorp.com
Bob	Chambers	robert.chambers@ferc.gov
Rod	Patterson	rnpatterson@midamerican.com
Laura	Hussey	laura_hussey@selgs.com
Bob	Chambers	robert.chambers@ferc.gov
Bryn	Wilson	wilsonwb@oge.com
Keith	Walters	step@eei.org

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

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

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

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

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

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

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

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

Preliminary, Draft, Unofficial Schedule for CIP-002-4

CIP-002 Task	CIP 2 Milestone Date	Week-of	Date	CIP-003 -- CIP-009 Task
		1/18/10		SDT Meeting - Work on requirement language
		1/25/10		sub-team meetings
		2/1/10		sub-team meetings
Informal Comment Period closes	2/12/10	2/8/10		sub-team meetings
SDT Meeting - React to comments		2/15/10		
Post for 45-day formal comment; form ballot pool	2/25/10	2/22/10		sub-team meetings
		3/1/10		sub-team meetings
		3/8/10		SDT Meeting - Work on requirements
		3/15/10		post initial unofficial draft (aid in CIP-002 ballot process)
		3/22/10		sub-team meetings
Initial Ballot start	4/2/10	3/29/10		sub-team meetings
		4/5/10		sub-team meetings
Initial ballot close; SDT Meeting - respond to comments	4/12/10	4/12/10		
		4/19/10		sub-team meetings
Recirc Ballot start	4/30/10	4/26/10		sub-team meetings
		5/3/10		sub-team meetings
Recirc ballot close; SDT meeting - respond to comments	5/10/10	5/10/10		
Re-recirc ballot start	5/16/10	5/17/10		sub-team meetings
Re-recirc ballot close; BoT Approval	5/25/10	5/24/10		sub-team meetings
File with Regulators	5/31/10	5/31/10		sub-team meetings
		6/7/10		SDT Meeting - Work on requirements
		6/14/10		
		6/21/10		
		6/28/10		
		7/5/10		
		7/12/10		SDT Meeting
		7/19/10		
		7/26/10		
		8/2/10		

CSO 706 SDT WORKPLAN TO DATE
OCTOBER, 2008 –DECEMBER 2010

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

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx
11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

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

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

12. July 13–14, 2009 in Vancouver, B.C., Canada

SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

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

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

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

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

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

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

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

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

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

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

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

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

CIP Version 3 Key Steps/Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 SDT Conference Call- Review of Industry Comments and Response**

3. **November 16, SDT 706 Meeting in Orlando, Monday, 5:00 p.m.- through dinner- SDT 706 Response Document to Industry Comments**
4. **November 17**, Tuesday, SDT 706 Meeting, Orlando, Complete and Adopt Industry Response Document.
5. **November 18**, Wednesday, Post Response Document and Ballot
6. **November 27**, Friday *(after Thanksgiving)* Deadline for Votes and Comments
7. **November 30, Monday, SDT 706 - Conference Call- finalize Industry Response document.**
8. **December 1- 10,** Recirculation Ballot.
9. **December 11,** BoT Approval
10. **December 29, 2009,** FERC Filing

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

1. **November 1:** Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP 002 Subgroups will form the CIP 002 Strawman Drafting Group (SDG).
2. **November 1:** All CIP 002 "meta groups" and subgroups will forward to the Strawman Drafting Group their standards text drafts including any guidance language**.**
3. Joe Doetzl will coordinate the work of the Controls Drafting Group (CDG) members: Jim Brenton, Keith Stouffer, Bill Winters, Jon Stanford. They will produce several recommended sample controls to illustrate high/medium/low concepts in CIP 002 as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a 'catalogue of security requirements', for circulation to the SDT **by Friday, November 13, 2009**.
4. The SDG will prepare a strawman draft by **November 13, 2009** for review by the SDT in advance of November 16-19, 2009 SDT meeting.
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and determine at the conclusion of the meeting if the SDT will continue to aim for the December adoption of CIP 002 draft on **December 16** for posting for industry comment.
6. The SDG and the CDG will present their 2nd drafts at a SDT conference call the **first week in December**.
7. The SDT will refine and circulate a strawman Draft #3 prior to the **December 15-16** SDT 706 meeting in Little Rock.
8. **December 15-16** will refine, finalize and adopt the CIP 002 posting for the industry.

- December 28, 2009 SDT Conference Call on CIP 002-4
- December 30, 2009 SDT Leadership Call- Security Controls Survey Draft
- January 6, 2010, SDT Conference Call- Review Security Controls Draft Principles and Schedule and Appoint Drafting Team to bring strawman to January SDT Meeting in Tucker.

CSO SDT 706 2010 MEETING SCHEDULE

18. January 19–22 — Tuesday-- Friday, Tucker, GA (GTC)	24. July 13–16, Tuesday-–Friday, Pittsburgh, PA (CERT)
19. February 16-19 Tuesday–Friday, Austin TX (ERCOT)	25. August 10--13, Tuesday—Friday, TBD
20. March 9–12 — Tuesday–Friday, Phoenix, AZ (APS)	26. September 7–10, Tuesday—Friday, Winnipeg, Canada
21. April 13–16 — Tuesday-Friday, Atlanta GA (SouthernCo)	27. Oct. 12–15, Tuesday-Friday, TBD
22. May 11-14 — Tuesday-Friday, Dallas TX (Luminant)	28. November 16–19, Tuesday-Friday, TBD
23. June 8–11 — Tuesday-Friday, Sacramento CA (SMUD)	29. December 14–17, Tuesday-Friday, TBD

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #5

Security Controls Sub-Team
Principles and Drafting Guidance

CSO 706 SDT SECURITY CONTROLS SUB-TEAM DRAFTING PRINCIPLES

(ADOPTED BY CSO 706 SDT, JANUARY, 2010)

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

SECURITY CONTROLS SUB-TEAM
PROCESS AND DRAFTING GUIDANCE AND DELIVERABLES

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

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

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

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

Appendix # 6
CSO 706 SDT DRAFTING SUB-TEAMS

Additional members may be necessary for teams that have a large number of requirements or FERC directives allocated.

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