Draft Meeting Executive Summary

Cyber Security Order 706 SDT — Project 2008-06

October 20, 2009 | 8 a.m.–5 p.m. CDT
October 21, 2009 | 8 a.m.–5 p.m. CDT
October 22, 2009 | 8 a.m.–3 p.m. CDT
Town Pavilion
1111 Main St.
Kansas City, MO 64105
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Meeting Summary Contents

EXECUTIVE SUMMARY

Jeri Domingo-Brewer, Chair, welcomed everyone and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines and also reminded the group of the sensitive nature of the information under discussion. The SDT adopted the August 10–11 and September 9–10, 2009 meeting summaries without changes or objection.

On Thursday morning, Jeri Domingo Brewer, on behalf of the SDT, thanked Kevin Perry for his service and contributions in building consensus and helping the team decode the cyber security puzzle as Vice Chair and presented him with a small plaque as a token of the team's esteem and appreciation for Kevin's dedicated service.

Scott Mix provided the team with an update on the TFE posting noting that all the regions have portals for accepting filings. He then reviewed Version 2 VSLs and VRFs noting it looks like it will be approved, which will close that group's work. The CSO706 SDT will be responsible for the VSLs and VRFs for Version 4.

Scott Mix provided an overview of the FERC Order on CIP version 2 and the procedural steps. He agreed to create a checklist of the over 200 charges from FERC Order 706 to help the SDT keep track of the milestones.

Mr. Bucciero summarized the effort to bring the team together in the interim to develop a rapid response process. The members discussed both the substantive issues with the interpretation of the term "auditably compliant" and with the SDT process for reviewing and voting on the response to the FERC Order. It was agreed that in the future the expectations should be made clear as to what the team is being asked to do and the communication process should be improved.

Scott Mix reported on the Standards Committee meeting and decisions regarding the response to the FERC Order and the CIP Version 3 next steps. Later in the meeting the SDT agreed on the following Version 3 steps and schedule:

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 Conference Call — Review of Industry Comments and Response**
3. **November 16 (5 p.m. through dinner) Meeting in Orlando — Response Document to Industry Comments**
4. **November 17 Meeting in Orlando — Complete and Adopt Industry Response Document**
5. *November 20 — Post Response Document and Start Initial Ballot*
6. **November 30 — Close Initial Ballot**
7. **December 1 Conference Call — Finalize Industry Consideration of Comments document**

8. *December 2–14 — Recirculation Ballot*
9. *December 16 — BOT Approval*
10. *December 29 — FERC Filing*

Scott Mix presented the "strawman" CIP-002-4 template format for the SDT's consideration. He noted that he incorporated the work done to-date by the subgroups into the document, and that the SDT and others should consider this very much a 'work in progress' subject to many changes between now and December 2009.

The subgroups provided progress reports to the SDT. John Varnell reported on the Reliability Functions Subgroup noting that they have not finished the definitions but hope to do so in the coming weeks. The members of this subgroup are also participating on three of the other subgroups.

Jackie Collett reported on the BES Subsystems/BES Cyber Systems Subgroup noting that they require more time to work and that in their last discussion the subgroup was stuck on "generation." She suggested that the SDT needs to think about all the components that are needed for each function. The subgroup was focused on multiple definitions of a BES Subsystem, and it has been using drawings to illustrate questions and guide discussion. Ownership of equipment has been another challenging question, along with who is responsible for paying to protect the equipment because it is critical. The subgroup hopes to resolve the first challenge during this meeting, but the second challenge may take more time.

John Lim reported on the BES Mapping Subgroup's progress noting that three subsystems were identified to map (generation, transmission, control center), but there was disagreement on this point. The subgroup spent time discussing scenarios related to high-medium-low impact levels and may need more than a high-medium-low in terms of effort and expense.

Phil Huff presented the report on the Cyber Analysis subgroup noting that they have all but eliminated the "target of protection" concept and centered discussion on BES cyber systems. The subgroup is exploring what potential functional impact the BES cyber system has on each of the associated BES operations and reliability functions. He noted that several definitions require additional work.

Keith Stouffer provided the report of the Definition and Selection of Controls Subgroup highlighting the control "template" format he has worked on with Scott Mix.

The SDT then had a full group discussion of the following topics:

- Number of impact categories and what that concept means — where to apply the reliability functions
- Linkage between functions and where BES mapping is headed

- High-medium-low definitions plus review of the two scenarios presented by Scott Rosenberger that focused on the amount of effort or number of controls required for each impact level
- Number of BES subsystems — how do you map the functions into physical assets you can assess and measure

The SDT discussion was wide ranging and touched on the following questions and topics, among others:

- As we develop formal requirements be careful not to simply create lists without a purpose — may be the first requirement is mapping of criteria and thresholds — allows for measurable standards for audit purposes
- Did we conclude how we would map cyber assets or categorize them into h-m-l based on functions? Level of combinations would be at the subsystem level — assign an impact level to the subsystem
- Trying to identify "juicy" targets — defining those is something we have to discuss and work out — do two mediums using the same asset raise it to a high or "juicy" level
- Any system supporting reliability should be part of the assessment process
- Expect the group to discuss and bring back a full set of requirements that take you from identifying cyber assets to full categorization
- What is "prescriptive" is in the eye of the holder — some need more detail to comply while others want more leeway to meet the standard
- Keep in mind how the entities would meet the requirement for an audit. May need to write the VSLs while writing the requirements

Following this discussion the SDT agreed to break into two "meta groups" that combined subgroups. One meta group combined the first three subgroups (reliability functions, BES subsystems/BES cyber systems, and BES mapping) and proceeded by moving through examples of generation and transmission, addressing the challenge of multiple owners, and working through the task of mapping functions. A second meta-group addressed the cyber analysis tasks focusing first on definitions, and then looking at reliability functions and impacts from the loss of integrity perspective, going back to the requirements language, and creating applicable guideline language.

The Chair presented and reviewed the schedule of activities for CIP version 4 and the FERC Order 706. The team discussed and tested a variety of options in terms of the pace of the schedule for producing the CIP Cyber Security standards and ultimately reached agreement on the following schedule:

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

The SDT agreed that the CIP-002-4 deliverables for posting for industry comment in December 2009 include the following documents: CIP-002-4 requirements and measures; related VSLs and VRFs; guidance document attachment to CIP-002-4; "Proof of Concept" controls (2-3 examples) illustrating the High/Medium/Low concept and the conceptual approach to replacing CIP-003-009; comment form with questions; and cover letter. The steps included:

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 the first four subgroups will forward to the SDG their drafts for the standards text, including any guidance language and the subgroups and meta-groups will be dissolved.
3. Joe Doetzl will coordinate the work of the Cyber Security Controls Catalog Drafting Group (CSCC) consisting of: Jay Cribb, Jim Brenton, Keith Stouffer, Bill Winters, and Jon Stanford. They will produce at least two examples to illustrate high/medium/low impact concepts as defined in the draft requirements of CIP-002-4, as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a catalogue of controls. These deliverables will be prepared for circulation to the SDT by Friday, November 13, 2009.
4. The SDG will prepare a strawman draft of the standard requirements and circulate it to the SDT by November 13, 2009 for their review.
5. The SDT will utilize the strawman draft to organize its November 16–19 meeting and reaffirm at the conclusion of the meeting if the SDT will continue to aim for the December 16th adoption of the initial CIP-002 draft requirements for posting for to the industry for comment.
6. The SDG and the CSCC will present their revised standards drafts during a SDT conference call the first week in December.
7. The SDT will refine and circulate a strawman draft following the December conference call but prior to the December 15–16 SDT meeting in Little Rock.
8. December 15–16, 2009, the SDT will refine, finalize, and adopt the initial draft CIP-002-4 standard text for posting to the industry for comment.

CIP Version 4 Key Deliverables, Steps, Schedule (January 2010-July 2011)

The SDT agreed that the CIP version 4 deliverables for initial posting in July 2010 include the following documents: initial draft of all the CIP Reliability Standards requirements and measures; VSLs and VRFs; guidance document attachment to the CIP version 4 standards; catalogue of security requirements; implementation plan; comment form with questions; and cover letter. The steps needed include the following with targeted completion dates:

1. January–June 2010: Develop 'catalogue of security requirements' as part of CIP Version 4

2. February–April 2010: Respond to industry comments on new CIP-002
3. July 2010: Initial draft of all CIP cyber security reliability standards prepared and ready for posting for industry comment as part of work plan, addressing all relevant Order 706 directives in a CIP Version 4
4. July 2011: Complete 3 Rounds of Drafts and Comments plus a final draft and implementation plan for balloting

On Thursday afternoon, the SDT identified and then discussed key open issues:

1. Better identification of reliability functions (BES cyber system identification based on reliability functions) — Meta Group 1 and 2
2. Better definition of terms used in BES mapping document: control centers/systems, generation systems, etc. — Meta Group 1
3. Cyber impact analysis alternative approaches and implications – avoid unintended consequences — Meta Group 2
4. Better sense of how all parts of the new standards fit together and how the entities will use it — reliability functions, where do they fit and how do you come up with cyber systems that apply — Meta Group 1 and 2

The Chair reviewed the next steps including the schedule for the version 3 response document and the CIP-002-4 effort. She thanked Joe Doetzl and Kansas City Power & Light for hosting the meeting and providing excellent catering and facilities.

The SDT adjourned at 2:45 p.m. on October 22, 2009.

MEETING SUMMARY

I. Introductions, Agenda, and SDT Work plan Review

Jeri Domingo-Brewer, Chair, welcomed everyone and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*).

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

The SDT approved the September 9–10, 2009 meeting summary without changes or objections. On Thursday morning Jeri Domingo Brewer, on behalf of the SDT, thanked Kevin Perry for his service and contributions in building consensus and helping the team decode the cyber security puzzle as Vice Chair and presented him with a small plaque with the following inscription: "Breakfast at Epiphanies — Leadership in Cyber Consensus — Kevin Perry, Vice Chair, CSO706 SDT, October 2008-October 2009."

BREAKFAST AT EPIPHANIES
Leadership in Cyber Consensus
KEVIN PERRY, Vice Chair, SDT 706
October 2008- October 2009

Scott Mix provided the team with an update on the TFE posting which generated the following comments:

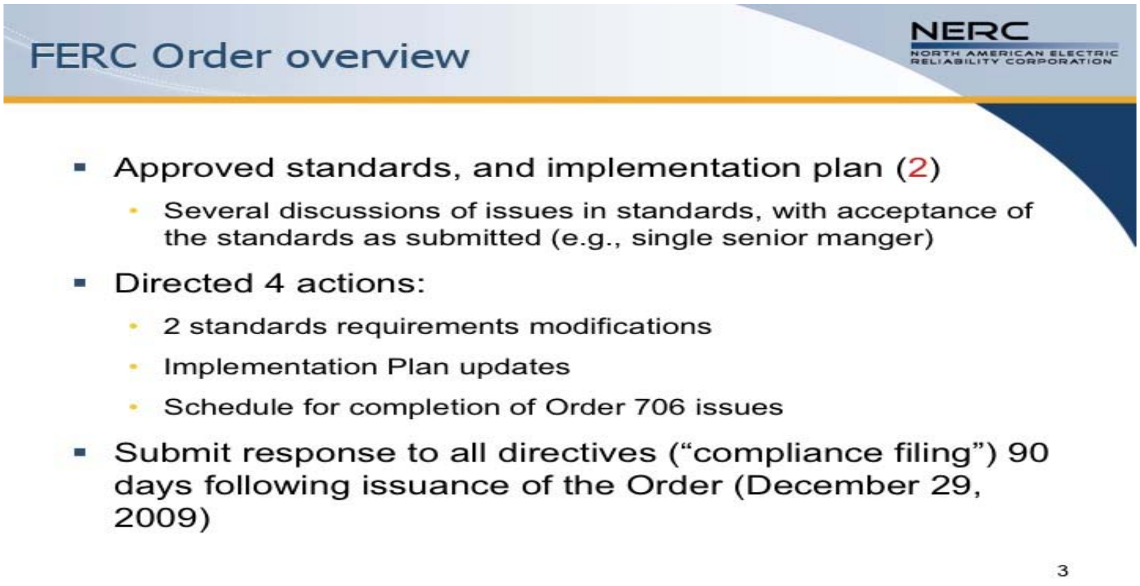
- Did FERC order say the TFEs did not need to be pre-approved? Yes, but they need to be pre-noticed.
- Will there be class based TFEs? Still debate about when it will appear and what it will mean — does not yet exist — still being discussed that may allow some form of pre-approval — question is what you will do to protect or mitigate and that cannot be pre-approved.
- All of the regions have portals for accepting filings.

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

II. FERC Order on CIP Version 2

A. Overview

Scott Mix provided an overview of the FERC order on CIP Version 2.



FERC Order overview

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

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

3

Member Comments on the Overview:

- When do we have to make the filing? (90 days — December 29th)
- Will they provide us with an attorney? Not clear
- Do we need to make the rule for Canada— not sure I can answer for Canada — NERC is required to file a response to the FERC directive by December 29th.

- Some of our work obviates some of the 200 but can we tell them we will not be done by December? The Order said “consider” not “adopt” the NIST standard — if adoption allows us to say we addressed the intent of the original order even if off in a different direction.
- Do we need legal assistance from NERC as part of this process to review? Do we need to integrate legal into the process? NERC is prohibited from developing the standard — does a legal representative blur that line?
- Mr. Huff addressed the time line not specifics of the order — a lot of details in how items are addressed over course of time – significant number of items to address – look at the 10,000 foot level first then zoom down as develop what the plan looks like.
- Concerned about legal input delaying the process – we debate the wording, legal would make that worse – Concerned with including legal in the standard development process — let NERC, FERC and industry legal review once the team has developed its response — let us develop the standards for protecting the system
- Maybe we need some substance expertise otherwise we may end up guessing in a limited time frame/
- In the past we had an electrical engineer/lawyer who helped with the wording — run the danger of letting them put in weasel words that dilute the product
- High level schedule discussed with NERC — (no, pulled from CIPC) — NERC is looking for this in formal form with more detail — (want to see a punch list for each item – this is an initial high level work plan — even this is very aggressive for developing consensus in the industry — need to discuss what is a realistic schedule because FERC will hold us to it)
- We need to do more to communicate to the industry on what we are thinking especially if we are accelerating our work — need to prepare the industry — make our meetings more efficient with substantive results — look into whether can we shorten the comment periods – communicate our direction early on
- For ballot period — ten days? How do we handle registration? (Not sure)
- Different team or us? (us – we will have to continue multi tasking)
- Looking for a spreadsheet punch list? We may not have an answer for every single one of the 200 items. What is required for the schedule response? What level of detail? What are the expectations?
- Mr. Huff offered a technical personal take — go through by subject area and group by subject — way to develop plan by subject areas with targets by areas — provides to industry and team the timeline for the plan)
- Some of our accounting may be that it no longer applies because of the approach taken — is that acceptable (it may be, given the approach you are taking)
- FERC Order punch list? Put on “parking lot”. Is that useful for keeping track of progress. Scott Mix offered to try to produce.
- Useful if we send out to the SDT (we have two that Scott developed – one takes the order and extracts out issues on what did FERC decided with several colors – the pieces were then put into a spreadsheet to follow how and when each dealt with, also included a high-medium-low value to the industry – basis for earlier suggestion for how to schedule

approach to responding to the items – low hanging first, then the 15 or so highest most important then the bulk of the medium neither easy or complex items)

B. SDT Rapid Response Process — Special Meetings and Electronic Voting — Joe Bucciero

Mr. Bucciero summarized the effort to bring the Team together in the interim to develop a rapid response process. The members discussed both the substantive issues with the interpretation of the term “auditably compliant” and with the SDT process for reviewing and voting on the response to the FERC order. It was agreed that in the future the expectations should be made clear as to what the Team is being asked to do and the communication process should be improved.

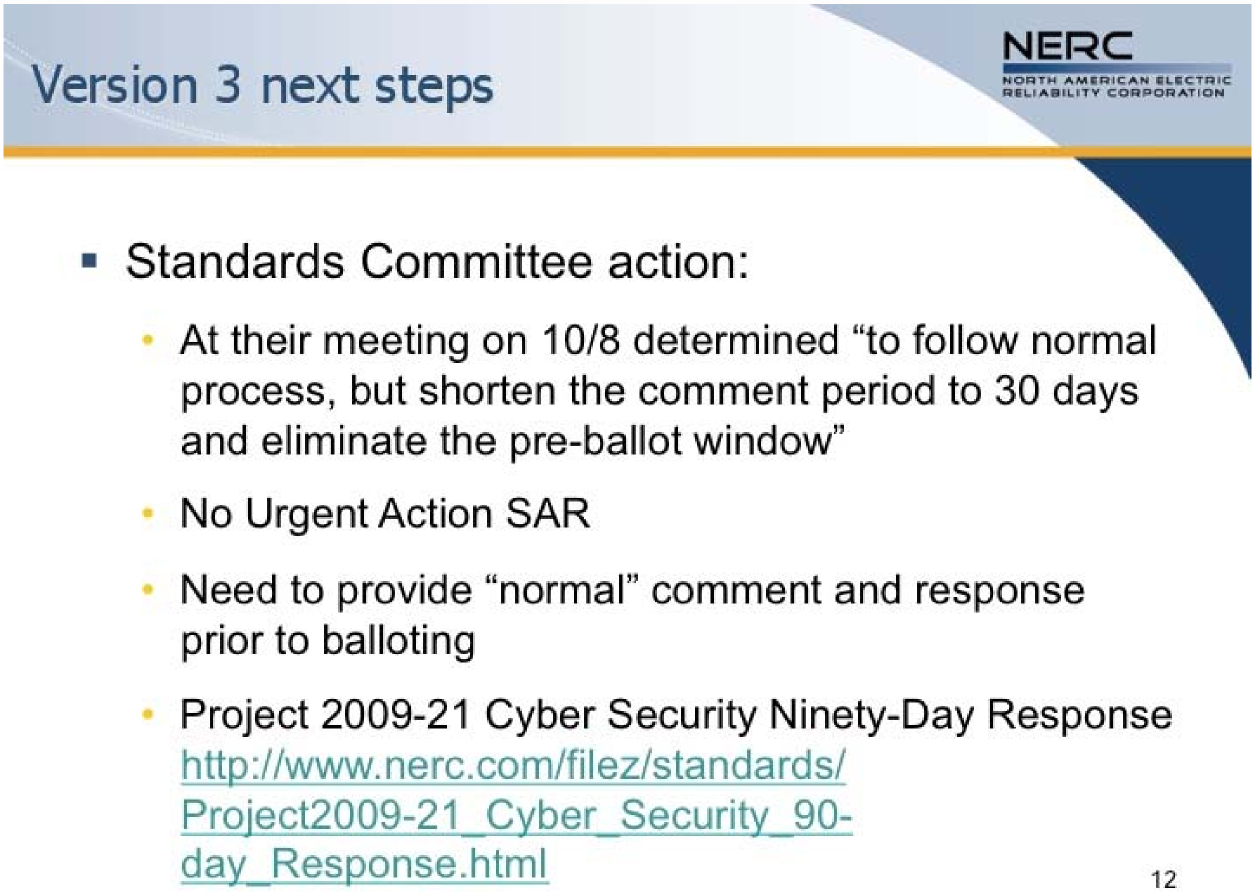
Workgroup Comments:

- We could/should have had a more transparent discussion than the last time – lesson learned, we need to communicate the discussion to the full group and the issues to be addressed
- We should have had a longer discussion to develop consensus before voting, especially the changes incorporated
- Many of the suggestions and additional change came after initial vote. Because of the rushed timeframe it was difficult to discuss those proposed changes and then revote.
- “Auditably compliant” has caused much confusion in the industry – many think it gives them an additional year contrary to what auditors think – compliant with full intent of the requirement and showing evidence of coming into compliance versus a year of data to show in full compliance – need to clarify the expectation going forward – this is important to Table 4 entities going forward and 2 and 3s carrying into a new year – to be fully compliant with intent you must conduct training – intent is that you do the action, not just periodically – collect logs for rolling last 90 days, maintain ongoing – if an incident (C date) then maintain for the past three years – you are compliant if you have the past 90 days – most disagreement centers around the periodic activity
- Did not get involved early enough – and then continued the discussion in the smaller group – question of what auditors are looking for – also difficult to get a full group together on such short notice, need sufficient lead time to include all – this was suppose to address the few issues FERC asked for - my concern was over the changes made after the team’s discussion, changes the industry might not agree with – that is a compliance issue that may belong somewhere else – industry balloted and approved, thus looking at a few changes and now asked to look at significant changes without sufficient opportunity to discuss – I disagree on the compliance interpretation and we will not have consensus – My real concern was how the process was handled
- What are the concerns about the interpretation?
- I think you have the year to come into compliance – access log check prior to compliance date? Moving up compliance actions before the compliance date – many on the team and industry have this concern – also sending something out to industry that changes something they already approved.
- “Auditably compliant” means you have a full year of data to support –

- I concur that we were codifying at the last minute a new interpretation of “auditably compliant” – many entities have a different view – need to put the issue over in the compliance interpretation section – this was not the time to codify especially on such a short discussion time frame.
- Three years ago tried to educate on the three levels of compliance in a series of workshops across the country – there is confusion on this issue – this issue clouds moving forward rapidly as required – need to be pulled out and dealt with separately – we are now exposed to negative responses – agree with Kevin’s interpretation and with Jackie’s view that it should have been dealt with differently and separately.
- Disagree with Kevin’s interpretation – requiring logs before the compliance date does not make sense.
- Our discussion should center around Table 2 compliance for new asset implementation
- There is no definition of “annual” from NERC
- The process and discussion could have and should have been handled better
- We can pull out the section from the ballot and NERC can put it out separately for comment since it is not under an urgent action order
- Compliance dates are based on when you wrote the procedures and when you started it
- Process lessons that we can apply going forward?
- Time to absorb and discuss, transparency of issues
- Decision on holding meeting on short notice was not taken lightly, but had no choice, only way to involve available members – it needed more time
- Even the limited opportunity for discussion improved the initial draft

C. Process and Schedule Going Forward

Scott Mix reported on the Standards Committee meeting and decisions regarding the response to the FERC Order and the CIP Version 3 next steps:



Version 3 next steps

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

- Standards Committee action:
  - At their meeting on 10/8 determined "to follow normal process, but shorten the comment period to 30 days and eliminate the pre-ballot window"
  - No Urgent Action SAR
  - Need to provide "normal" comment and response prior to balloting
  - Project 2009-21 Cyber Security Ninety-Day Response http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

12

Later in the meeting the SDT agreed on the following Version 3 steps and schedule:

Version 3 Key Steps and Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 Conference Call — Review of Industry Comments and Response**
3. **November 16 (5 p.m. through dinner) Meeting in Orlando — Response Document to Industry Comments**
4. **November 17 Meeting in Orlando — Complete and Adopt Industry Response Document**
5. *November 20 — Post Response Document and Start Initial Ballot*
6. **November 30 — Close Initial Ballot**
7. **December 1 Conference Call — Finalize Industry Consideration of Comments document**
8. *December 2–14 — Recirculation Ballot*
9. *December 16 — BOT Approval*
10. *December 29 — FERC Filing*

III. CIP 002 Strawman

A. Overview of CIP 002 Strawman Template

Scott Mix presented the “strawman” CIP-002 template format for the SDT’s consideration. He noted that he incorporated the work to date of the subgroups into it and that the SDT and others should consider this very much a work in progress subject to many changes between now and December, 2009 (See Appendix # 5)

Member Comments

- Regional entity is a statutory requirement
- RRO does not exist anymore
- Because it was confused with RRE – that needs to be fixed
- New entity – RRA – we could break new ground and include
- In the narrative spell out interconnection variances – are they regional or should they be up in the standards (there is a number for the east, the west, etc., it is in the language of the requirement)
- For the interconnection is there a designation for the authority separate from the region? (East is a split authority)
- Good value added with the template

B. Subgroup Reports to the SDT

1. Reliability Functions Subgroup Report and Key Issues and Draft CIP 002 Language

John Varnell reported for the subgroup noted they have not finished the definitions but that should not hold the rest of the team up in moving forward. They have shared their initial work with other teams and the members are participating on the other 3 teams.

Member Comments

- Time frame for finishing the definitions? A couple of weeks
- Will this be published with the standards?
- Definitions do not affect what is being done on the other teams but how people will interpret so may be part of the filing, maybe as a FAQ or guidance document.
- This is an area where group may blaze new ground – may want to make part of standard to give it more weight than just a FAQ – consider a guidance document.
- Reliability functions – make those the basis for guidance to the functions

2. List of BES Subsystems/BES Cyber systems Subgroup Report Key Issues and Draft CIP 002 Language

Jackie Collett reported on the group’s progress noted they require more time to work and that in their last discussion the subgroup got stuck on “generation” – we need to think about all the components that are needed for each function. Next conversation focused on multiple definitions of what a BES system is and they have been using drawings to illustrate questions and guide discussion. Ownership of equipment has been another challenging question and who is responsible for and paying to cover them because they are critical. The subgroup hopes to resolve the first element while here but the second element may take more time

SDT Member Comments

- Group 1 and 2 need some in depth discussion together. They will meet together this afternoon.

3. BES Mapping Subgroup Report and Key Issues and Draft CIP 002 Language,

John Lim noted there were three subsystems to map and there was disagreement on this point. The subgroup spent time discussing scenarios related to high-medium-low impact levels – may need more than a high-medium-low in terms of effort/expense.

Member Comments

- We need to communicate together as a single group this afternoon rather than as subgroups- need to be sure we are on the same page rather than four or five groups doing distinct things
- May be premature to consider until we finish the sub team reports – will revisit after lunch and the rest of the reports

4. Cyber Analysis Subgroup Report, and Key Issues and Draft CIP 002 Language

Phil Huff presented the report on the Cyber Analysis subgroup noting that they have all but eliminated targeted protection – and centered discussion on BES cyber systems – reliability function assessment assesses the potential function impact the BES cyber system has on each of the associated BES operations. He noted that several definitions require additional work and more eyes (review) from others – protection of the system relies on the definitions and reliability functions. He also noted that they need more time as a sub group on definitions and for input form other groups too

5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP 002 Language

Keith Stouffer provided the report of the subgroup, noting the control "template" he has worked with Scott Mix on in terms of an acceptable format.

Member Comments

- How do we break this into l-m-h and for different systems? –generation, control and transmission?
- Estimated time needed? Maybe four or five years or within the time we have available.
- We will need more time to build common consensus in the group as a whole.
- Also need to run this format by the NERC staff
- This is just one requirement as an example – we will divide the group up to deal with the rest of the requirements.

- Need to be sure we are not continuing on the path where we are split up just to support and continue the process – we need to get back together as a whole to deal with key issues sooner rather than later
- This can be posted as an example of applicability – we will need to do a good job of communicating to the industry that this is an example and not asking for their comments in detail

C. Key Issues Going Forward.

The Chair and Vice Chairs tested whether to break into small groups or stay together to identify and document the several key outstanding issues to be addressed. The group suggested a full group discussion of the following topics:

- Number of impact categories and what that means – where to apply the reliability functions
- Linkage between functions and where BES mapping is headed
- High-medium-low definitions (first)
- Number of BES subsystems – how do you map the functions into physical assets you can assess and measure

1. High-medium-low definitions

Member Comments

- Do members have a notion how big each category is? – does low represent 50% of the assets? More or less than that? Is high equal 5 or 10 % of the assets? That may drive some of the criteria thresholds.
- Will have to meet the low standard for everything – the medium and high will require more.
- Do we need a category below low, such as none?
- No need for something below low – prefer scenario 1 with some adjustment of the percentages.

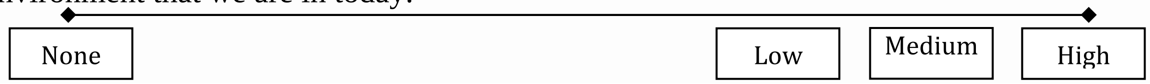
Conceptual discussions related to High, Med, Low Impact Levels (Scott Rosenberger)
There were many comments related to the adequacy of 3 levels of impact presented in our concept paper. Some of the need to suggest the possibility for the need for additional levels of impact stems, in my opinion, from the lack of clarity as to what the amount of effort or relative number of controls are associated with each level.

Scenario 1

Impact Level	**Low**	**Med**	**High**
Amount of effort/Number of controls (compared to High)	60%	80%	100%

In this scenario, it is arguable that a Lower than Low is necessary as Low requires significant effort to accomplish (Low is not Low Effort). In this scenario, Lower than Low then turns into

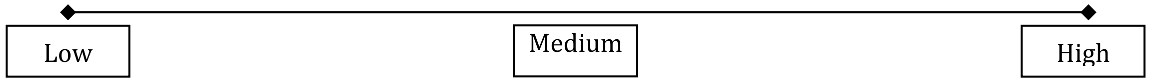
0% (or no impact, no controls) and this scenario looks conceptually like the all or nothing environment that we are in today.



Scenario 2

Impact Level	Low	Med	High
Amount of effort/number of controls (compared to High)	10%	50%	100%

In this scenario, there is a significant difference in the effort/expense required for the three impact levels. A case could be made that most if not everything would at least fit into the low category. With the major focus being re-directed to the identification of Medium and High impact areas.



A significant benefit of Scenario 2 is that more Security work would be done on more assets and there would be few (if any) that have nothing done and would make the effort/expense required (Low) commensurate with the risk (Low). The industry could then focus on protecting those BES Subsystems that have a more significant impact to the BES

- Scenario 2 concerns me – the compliance load on the entities – requires documentation on every element of the system – 75% in the low would still require 90% of the compliance effort – prefer recognizing some will need little or no effort for compliance
- Need to determine how much is in each category – need something less arbitrary – how much is in each bucket?
- John Lim’s group on the BES mapping only came up with the high and medium, everything else was put in low – the point here is determining what is low
- Scenario 1 allows for none
- Can reliability requirements deal with issues in generation
- Feedback form concept paper asked why we were going to this categorization of h-m-l – the high and medium were easy, low was everything else – low should be a low amount of work even if the largest category
- The concept reflects a cost perspective? Will groups simply assume everything should get a high level of protection to avoid liabilities?
- How big is the compliance requirement for those in the low category? Are there parts of the system that require little or no protection and thus lower than low?
- Every entity still has assets that have nothing to do with BES but will need to categorize them for auditors – they may have their own protection systems – you have assets that do not need cyber protection
- Careful that even the most remote part of the system if connected leaves the system vulnerable

- Prefer numbering rather than h=m=l which would require putting something in the buckets – industry might be more open to level 1, 2, or 3 of impact – there are assets out there that do not need anything because they do not have an attack vector
- Focused on BES elements or cyber assets? Does it matter? It does in my world
- NERC has statutory authority only over bulk electric system assets – not distribution or marketing systems
- But how do I group the assets and their functions in a control center?
- In the federal system, every single system has to have minimum level of security
- Few assists in the high, some in medium with the bulk in the low categories of impact – don't need many controls to protect the low, concern should be for protecting the high and then the medium – the three levels help direct the limited resources to ensure the most bang for the buck
- Functions define what you look at first for coverage – this is a penalty standard, a list of what you will be penalized for
- Yes, focus on the areas of the most risk – prefer scenario 2 because it allows focus on the highest risk and not on the lowest
- We are trying to minimize the risk to our company – we need to keep the focus on the security of the system in the most cost effective way possible – need to work on security, rather than on compliance
- Are we protecting all BES systems?
- Different systems balance the functions – how important is a subsystem to a function?

2. BES Subsystems

- Use an example of generation subsystem – for purposes of discussion – individual units may not be high – but may be as part of the larger system – look at it from a reliability requirement from different perspectives.
- How would requirement do that? How many steps would it take to cover all of the possible scenarios or related systems?
- You have to have the flexibility to address different subsystem configurations. The configurations could be in the hundreds
- Take them all in common, not necessary to figure out all the possible configurations – because you have the flexibility, the more reason to consider them collectively
- We have to determine the common elements. Need to work from the big down, not from the subsystem up – should not have to work through all the possibilities – the intent should not be to determine what is a requirement and how to avoid it but how to protect the highest priorities.
- Focus on the facility – don't have to focus on the whole facility just because it has one black start.
- Concerned about this slicing and dicing approach – what is the total generation from the facility and the functions – I don't see value in grouping elements.
- It is a requirement to look at it in multiple ways – analyze as a unit and a facility?
- Need definitions to be flexible.

- It is not flexible but rather prescriptive
- Industry needs an analytical approach with criteria for impact levels
- Need to focus on the facility as a whole and the subparts only as needed – suggest moving discussion toward functions
- Reading too much into the diagram

3. Reliability Functions:

- Need to look at how the functions impact the other groups.
- Look at where to apply the reliability functions as a basis for cyber security impact identification.
- Use as a basis for defining or identifying BES subsystems; the components that need to be defined -
- The performance of these functions is what has impact – have to protect the function rather than the asset.
- Define subsystems based on the reliability function they perform or support.
- We protect assets because they perform reliability functions – we protect transmission because it moves power from generation to consumption – which ones and how much depends on importance to the reliability of the system. That's why we split this up by function.
- I like the approach that looks at what we think the answer should be – start with the end in mind.
- If we start with the BES subsystems, we are starting in the middle – we need to start at the top, most important and work down.
- The control center is the physical building. Not everything in that center is essential to the function you are trying to protect.
- The control center is not a subsystem - we need to be careful how we use the words.
- Control center as a building is less important – talking about two different things – cannot possibly define everything into three subsystems.

4. General Discussion of CIP 002 Issues and Strategy Going Forward

- Need to determine what we need from groups to go into the requirements – first get list of BES systems, take that list and define its impact – what are we looking for? A requirement that says entity list their BES systems or say what kind of subsystems they are – guideline for determining function of the subsystem?
- Apparent yesterday we are not coordinating on BES subsystem versus subsystem – function or component to complete the task – each entity creates list of subsystems of items needed to perform a function or task.
- In categories we have special category for special subsystems – include subsystems that are not related to specific pieces of hardware but perform a BES function

- As we develop formal requirements be careful not to simply create lists without a purpose – may be the first requirement is mapping of criteria and thresholds – allows for measurable standards for audit purposes –
- Cyber Analysis subgroup might begin developing language this afternoon for full group to look at.
- Did we conclude how we would map cyber assets or categorize into h-m-l based on functions?
- Level of combinations would be at subsystem level – assign an impact level to the subsystem
- Trying to identify "juicy" targets – defining those is something we have to discuss and work out – do two mediums using the same asset raise it to a high or "juicy" level
- Still thinking electric grid not security – can kill a "juicy" target from a non-juicy source – control system is an overlay from a different plane than reliability of the electric grid
- Any system supporting reliability should be part of the assessment process.
- John Lim noted that what we have needs to be vetted by the full group – be sure we are on the right track – but how do we apply, either as a standard or second document – do we need a list for requirements guys or is the functions the categorization the list
- Three groups need to get together to determine what is in the standard – what are we asking the entities to do?
- Still confusion on what each needs to bring back for the standard and the support document
- Do the groups need additional input from the whole team as to what is expected?
- Expect our group to discuss and bring back a full set of requirements that take you from identifying cyber assets to full categorization
- Rich reviewed a rewrite of the language for the functions list and the impact value
- As we break to write requirements – keep in mind, 65% of requirements were prescriptive or administrative – stick to what's not the how's
- What is "prescriptive" is in the eye of the holder – some need more detail to comply will others want more leeway to meet the standard
- Keep in mind how your entity would meet the requirement for an audit
- May need to write the VSLs while writing the requirements

D. "Meta Groups" Meetings and Reports

Following this discussion the SDT agreed to break into two "meta groups" that combined subgroups.

1. Meta-Group #1 (Subgroups 1, 2, and 3 jointly met)

Scott Rosenberger suggested taking one of the functions and run through an example of how it would be implemented in the BES Mapping and BES Subsystem subgroups. Below are comments both in plenary and the meta subgroup:

- **Working through Examples.** Spent time identifying which reliability functions went with which mapping criteria – need more time to work through examples. Thought I would take generator than met one of four then look at cyber functions identified for protection. Too many "can't be done" answers at the end – not sure what are the next steps/

- I learned the value of an example – thought we had agreement but then differences arose when we tried out an example.
- A few things came out – we made certain assumptions, taking into account the functions in looking at mapping criteria – We brought Phil in for some clarifications, found he was working based on clarifications of functions – pointed out the need to reconnect the criteria to the functions to begin bridging efforts – good start toward bridging in the future –
- Also, if you have a high on two different criteria, what happens then?
- We tend to bog down in the weeds – this prevents us from trying some things – eventually we may need to press through and ask for industry comments to help identify where clarifications are needed.
- Do we need a broad general definition?
- **Multiple Owners.**
- Different owners in the same subsystem – how do we tie them together?
- Multiple owners of subsystem is still concern.
- Some of the categories in the mapping we have to be able to say what is the generation subsystem – focus on what makes sense for generation subsystem rather than the ownership
- Concerned about using terms "transmission" or "control center" – change latter to control and operate function?
- **Generation**
- Look first at generation and transmission – have some drawings we can talk from – what is a generation subsystem? How does it relate to the BES function and or mapping?
- Those are filters to determine its impact on the system – if it is taken away what is the impact on the function
- Some of that is built into the criteria – some of the criteria addresses some of the functions
- Your list has seven functions related to the generator
- Those operating the transmission system don't care about most of these functions.
- How does BES cyber system affect the reliability function? The matrix tells you how the reliability function impacts.
- High impact generator – do any cyber systems affect that generator? It is on my BES mapping and is "high" – how do I determine what to protect?
- Impact based on security criteria not on impact on the BES
- **Functions and Mapping**
- Do we need to describe what the BES subsystem looks like for each of these functions?
- Same components for each of these functions? Many may be the same.
- The way you use the function is based on the criteria used to determine impact.
- Are we going to have a generation mapping and one based on reliability? Reliability overshadows all of the mapping pieces.
- Does mapping we already do that?

- There is not a direct mapping between reliability functions and subsystems. Instead functions are the underlying information for the impact criteria.
- This is an exercise to be sure reliability is mapped and accounted for
- Phil's group should come up with criteria related to reliability of cyber system
- He is looking at which application, not the same as BES big iron things
- Functions are used to define impacts – three definitions
- Subsystems are building blocks for criteria
- Phil Huff suggested that you assess cyber systems based on reliability functions – combine impact criteria.
- How does cyber system impact or perform reliability function? Can I do the function without that system?
- Come up with matrix to be sure the correct relative rating and appropriate controls
- Incredible amount of minutia to document and lots of "phrasing" of the considerations.
- Are we making this overly complicated? Today, we determine if you have a critical asset then look for all the systems that impact that asset, analyze it for all the criteria, look at the critical aspects for protection/
- Trying to write the CIP standard(s) less prescriptively
- A BES subsystem is not just big iron.
- Phil's group is going through the cyber system side and others are trying to go through the BES subsystem mapping – later work together to reconcile the two sides.
- If not defined by NERC reliability standard as criteria.
- Can have a "high" on the mapping side but a medium on the cyber side. The "High" water mark makes it high for both.
- Have to list the cyber systems that support the BES system function.
- Use the blue side (cyber asset) for those without the bulk electric generation assets.
- Generation, transmission, control and special systems – four areas for definition.
- Next: review functions first, then look for how mapping ties to functions
- In terms of function – what's missing?
- Talking about an automated real time response – "dynamic" response
- We walked through this as a group and added which function applied to BES mapping criteria

2. Meta Group #2 – Cyber Analysis and Controls Subgroup

Phil Huff noted they would be working on definitions and looking at reliability functions and look at impacts from loss of integrity. The may need to go back to the requirements language – and create guideline language – Are the standards ready to be combined by the end of this meeting? Concern with the BES mapping and what is in the standard or not.

Comments

- How should the list of functions from Varnell's group be handled and how they relate to the BES subsystems? Went back and looked at definitions of what is a cyber system and what is BES system. Then looked at the cyber analysis piece

- No true consensus yet on approach
- Map out the BES systems before doing a cyber analysis.
- Phil reviewed language changes in the draft document.
- Challenge to marrying things together in the lookup table
- Requirement 5B an alternative solution – using the BES mapping table – we need feedback from the full group – how do we get to the final picture? Is this an easier way to go?
  - Walk us through 5A?
  - Identify BEX subsystems through which the cyber system supports or has potential to impact reliability functions
  - Then assess the potential function impact the cyber system has on each of the BES subsystems – under Reliability function assessment
  - BES system mapping just associates or relates the cyber systems to the BES system
  - Does the scale of the generator play into the analysis?
  - No
  - Then you are double loading the cyber analysis process – the cyber impact is the same for big or small generator, but the BES analysis is different for each – will end up doubling the work
  - When you look at cyber system it is done once for the BES system
  - As an auditor I may expect to see what is the impact of each cyber system on any associated BES systems
  - Have not considered different BES cyber system categories
  - But the auditor is going to ask for a unique identifier for each cyber asset
  - Map device to specific BES subsystem and look up the impact – puts it into a sequential process rather than two parallel process that meet at the end
  - Should be able to take advantage of commonality of systems to do one analysis for economy of scale
  - The pieces may not be high but the system as a whole is high
  - How do you handle systems that talk IP up one system but not others?
  - That is a separate issue – just because data is exchanged or talking by IP does not mean it is attackable
  - BES mapping – 5B means is there anyway to make the cyber system cause high impact (3.1.1-4) then it is high – puts a big onus on defining your subsystems.
  - We should only care about systems that affect the BES not minor subsystems – suggest you check BES system first before checking the cyber system.
  - The only difference is that the medium and low are taken out of the analysis.
  - Look at BES systems first – they are going to look at the generator first, the control system, because they have the tools to do that.
  - Tighten up what we mean by a system – no single relay works by itself – do we need to qualify a system by the fact it communicates.
  - You may have to both – look at it from both perspectives – neither the green or blue side is correct alone – don’t spend our time deciding which is right but work through examples.
  - Difficult to come up with something demonstrable and repeatable for an auditor – trying to do analysis once, not repeat it for both sides.

- If do BES system you knock out most and only do analysis of cyber systems related to those identified the BES system side.
- Doing separate analysis then trying to bring together is unnecessarily complicated
- As a company that cannot control the other end then I need to protect myself and my partners
- We have to look for the solution that covers the lowest common denominator
- Our group concluded that whatever h-m-l rating comes out we will apply – concerned about integrated systems that may be vulnerable to entry from the low side
- The highs are easy to identify but more difficult to identify lows that may allow access to the high or critical systems – but I can only control my equipment, I have to limit the attack vector by how I set up my "high" equipment
- The focus needs to be on what affects the BES
- Even the low may need some substantial protection if it talks up line
- The 5B approach captures the current gap which is aggregated BES subsystems where they were identified as low – still needs protection
- Look at potential span of control – what is the scope or range of control – iterative analysis or process–
- How do you write a requirement that allows for a high to change to medium where appropriate? If possible that would address much of my angst
- Getting into the weeds again – in terms of definition of boundaries

IV. CIP Review Milestones and Schedule

A. CIP Version 3 Key Steps and Schedule

The Chair presented and reviewed with the SDT the schedule for Version 3 and the FERC order discussed and agreed to on the first day (Tuesday):

1. Post for Industry Comment 10-13-09 to 11-12-09
2. **November 13 Conference Call — Review of Industry Comments and Response**
3. **November 16 (5 p.m. through dinner) Meeting in Orlando — Response Document to Industry Comments**
4. **November 17 Meeting in Orlando — Complete and Adopt Industry Response Document**
5. November 20 **—** Post Response Document and Start Initial Ballot
6. **November 30 — Close Initial Ballot**
7. **December 1 Conference Call — Finalize Industry Consideration of Comments document**
8. December 2–14 **—** Recirculation Ballot
9. December 16 **—** BOT Approval
10. December 29 **—** FERC Filing

B. CIP Version 4 Key Steps and Schedule

The team discussed and tested a variety of options in terms of the pace of the schedule for producing the final CIP 002-009 and ultimately reached agreement on the following schedule:

1. CIP 002-4 KEY STEPS/SCHEDULE (OCTOBER-DECEMBER, 2009)

The SDT agreed that the CIP-002-4 deliverables for posting to the industry for comment in December 2009 include the following documents: CIP-002-4 requirements and measures; related VSLs and VRFs; Guidance document attachment to CIP-002-4; "Proof of Concept" controls (2-3 examples) illustrating the High/Medium/Low concept and the conceptual approach to replacing CIP 003-009; Industry Comment Form with questions; and Cover letter. The steps included:

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 the first four subgroups will forward to the SDG their drafts for the standards text, including any guidance language and the subgroups and meta-groups will be dissolved.
3. Joe Doetzl will coordinate the work of the Cyber Security Controls Catalog Drafting Group (CSCC) consisting of: Jay Cribb, Jim Brenton, Keith Stouffer, Bill Winters, and Jon Stanford. They will produce at least two examples to illustrate high/medium/low impact concepts as defined in the draft requirements of CIP-002-4, as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a catalogue of controls. These deliverables will be prepared for circulation to the SDT **by Friday, November 13, 2009**.
4. The SDG will prepare a strawman draft of the standard requirements and circulate it to the SDT by **November 13, 2009** for their review.
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and reaffirm at the conclusion of the meeting if the SDT will continue to aim for the December 16th adoption of the initial CIP-002 draft requirements for posting for to the industry for comment.
6. The SDG and the CSCC will present their revised standards drafts during a SDT conference call the first week in December.
7. The SDT will refine and circulate a strawman draft following the December conference call but prior to the December 15-16 CSO706 SDT meeting in Little Rock.
8. **December 15-16**, **2009**, the SDT will refine, finalize, and adopt the initial draft CIP-002-4 standard text for posting to the industry for comment.

2. CIP VERSION 4 KEY STEPS/SCHEDULE (JANUARY, 2010-JULY 2011)

The SDT agreed that the CIP Version 4 deliverables for initial posting in July 2010 include the following documents: initial draft of all the CIP cyber security reliability standards requirements and measures; VSLs and VRFs; Guidance document attachment to the CIP Version 4 standards; catalogue of security requirements; Implementation Plan; Industry Comment Form with questions; and Cover letter. The steps needed include the following with targeted completion dates:

1. **January - June 2010**: Develop 'catalogue of security requirements' as part of CIP Version 4
2. **February- April 2010**: Respond to industry comments on new CIP-002
3. **July 2010**: Initial draft of all CIP cyber security reliability standards prepared and ready

for posting for industry comment as part of workplan, addressing all relevant Order 706 directives in a CIP Version 4.

4. **July 2011**: Complete 3 Rounds of Drafts and Comments plus a final draft and implementation plan for balloting.

Member Comments on the Schedule

- Unless team changes the current schedule, CIP Version 4 will have to be completed in 13 ½ months.
- Complete generation of catalogue controls is a huge task. Even reaching agreement among the SDT, we won't get industry to agree by balloting. Current draft schedule only has 2 rounds of comments built in to it. With 45 days for each.
- For Version 1- the SDT had conference calls every day for months. What is a reasonable number of rounds of member comments?
- Process vs. calendar base. Set a calendar and modify process? Can't do both.
- Need to say more than just four rounds without giving some times certain.
- We need to guard against rushing it out and not having a good product – schedule should be industry approval plus one or two months – if that is not good enough, let them give us a deadline – As much as I would like to, I am not optimistic we can get in done by Dec. 2010 – we cannot control industry comments and the number of ballots needed for approval.
- Here is what we think it would take to address issues – if industry says more work is needed then schedule could go out additional months.
- The critical date is draft one – does our current process allows us to get it out by Dec 2010?
- We have a defined process for Dec 2010 and the final approval but the middle is squishy
- Assume two cycle schedule and industry may require more – we can agree how long a cycle will take but not how many cycles will be necessary – two cycles is a good WAG
- Two cycles is optimistic given the changes we are suggesting to the regulatory environment – past efforts needed four cycles without the regulatory element – here we need four cycle minimum.
- Clarify ballot versus comment cycles – we are talking about post/comment cycles before sending to ballot.
- FERC says okay to our suggestion but do they leave a disclaimer to modify their order if needed?
- I would like to think we could file an amendment to add cycles based on industry comments as documentation.
- Concerned we will file a schedule with best estimate and it will not be politically acceptable – FERC will say accept but shorten time period.
- There is a perception or concern we are already late – the industry is just frittering away time – also depends on quality of comments – go as far as we think we can get away with, that may be first quarter of 2011 – what can we get without tipping it over – intuition says three cycles and first quarter 2011
- Others have taken five revisions over five years – precedent with standards that are not as complicated.

- Markey has hearings next Tuesday and plan to talk about how fast we are moving – high visibility issue.
- We are responsible for producing under the issues – function in the environment we are in –
- Do not believe Dec 2010 is achievable, question if Dec 2011 is achievable – have we addressed requirements put forth by the FERC? Do we quickly address the order, throw it over as version 4, then take time to address broken standards – this might get FERC off our back, may defer Congressional action too.
- Willing to think FERC is thinking about how we address the 706 requests – political reality will say get it done.
- Anything interim may help with FERC but not the politics – anything that hints at a redo or makeup will not sit well.
- The cantankerous Canadian view – impression from up north, we are doing a lot of second guessing – do what we think we need to do, a realistic schedule – band-aids will not serve the industry well – band-aids will not work with the industry, they want a fix – our role is to support the reliability of the BES
- Concern is founded in CIP8 where we thought we were doing what they asked and they did not approve – can we address all the issues within the proposed timeline? Would like to think all the issues will be addressed in the complete rewrite – how much are we going to have to do to address confusion in the industry? Does paragraph 25 require three levels of control? Applicable features of the NIST framework? We have to do our best to find door out of the dark hallway – this is the only process we have to get it done as quickly as possible – these standards were never designed for “smart grid” – not our job to address it now – focus on “addressing” the NIST framework.
- Focus on what is it we have control over? Some issues FERC will come back and clarify for us – cannot focus on what we think they want – do the best we can to give an estimate what we need to get the job done, caveat with maybe issues out of comments that may need more time – best estimate given what we know now.
- Number of issues up for interpretation – more issues are clear, don’t need clarification and must be addressed even if concern is no longer applicable because of other changes suggested – have a good answer for each item
- Sent out matrix Scott and the Chair worked on with magnitude column – VH are the very high that may not fit in Version 4 – items that may require a V5.
- Now for the wake up call – testimony for Congress next week – NERC general counsel saying we will be done middle of next year, not even Dec. 2010
- We have the attention of the industry – shorten review cycles to 30 days – helps buy some time?
- All choices assume draft by April? Just a matter of how many cycles? Still need to discuss getting draft by April 2010
- Assume draft ready by April 2010? If so, then choice is between how many cycles
- Suggest when we think full package ready for post – beyond that why vote on how many cycles it will take?
- Because FERC asked – and NERC wants/needs to know what the estimate is.
- Nailed down realistic time frame for complete package for posting rather than ballot – currently April 2010.

- Optional dates for posting draft
- Realistically we will need time to respond to CIP 002 comments – amount of work putting together catalogue represents a shift in the industry paradigm.
- However we have resources and we are not reinventing the wheel.
- Did not consider the cycle of comments when I suggested July
- Should we put in cycles?
- This is a draft of the whole CIP 002-009?

Straw Poll- Date for First Full Draft of CIP 002-009

Date	April	July	October	January 2011
Member Votes	3 votes	10 votes	3 votes	3 votes

Member Discussion of Straw Poll
Comments of those favoring April 2010

- I was trying to keep us on schedule for NERC and Congress
- Feel the controls catalogue piece will go faster than you think
- Need to draw line in sand to shoot for

Comments of those favoring July 2010

- The line in the sand is when we will be done with CIP002 – how soon will we get there?
- JB: more realistic – April is not realistic given the way we have been working - do think catalogue will go quickly but still need enough time to reshape the wheel

Comments of those favoring October 2010 and January 2011

- SDT will need time to rewrite controls carefully and will need time to respond to industry comments
- We can make April 2010 if we restructure the SDT effort – want to discuss restructure to make that date – only voted October as realistic for how we operate now
- Does this proposed schedule include what Scott Mix calls the very high “uglies”?
- Some of those “ugly” issues are not addressed by this group.
- If the issues are in the 706 order to be considered and relate to CIP – can’t ignore it.
- Directives in 706 presupposed no radical changes to standards – as we radically change standards then many of FERC concerns may no longer be applicable – the current standards are fatally flawed and need more than band-aids – but a new set thrown over the wall, FERC may say did not respond to directives.
- Need to make sure that if there are FERC 706 issues not even addressed by the new approach, we know that sooner than later.
- Need to address serious issues that are not covered – also, we can claim meet 18 months if draft ready by July 2010 – look at two tracks: 1) control or data center and 2) field sites – more pain in the latter, but may address some of this with a separate additional effort looking at physical security.

C. SDT Structure and Deliverables Challenges

The SDT CIP-002-4 deliverables for posting in December include:

- CIP 002 requirements and measures,
- VSLs and VFRs
- Guidance document attachment – CIP-002-4
- “Proof of Concept” controls (2-3) illustrating the High/Medium/Low concept and the conceptual approach to CIP 003-009.
- Industry Comment Form with questions
- Cover letter

The SDT considered the following proposal:

By November 1 the current 5 subgroups will produce final thoughts for the new drafting teams, and then dissolve. A lead drafting team would be formed from current chairs. A catalogue of controls group would work on the 2-3 controls. In January, 2010 may need to re-divide to conquer on parallel paths: 1) Need more eyes on the controls for development of the controls language volunteers: Joe Doetzel, Jay Crib, Bill Winters(re-volunteering), Jim Brenton

Member Comments on the Proposal:

- Instead of four groups continue with the two groups formed yesterday to conclude by November 1?
- Concerned with what Keith Stouffer is doing – like to revisit – need to rationalize the 15 issues across the standards
- Still talking about creating an example of CIP5 – access control
- Looking at it from a functional model using other standards as potential entry points – and working with Scott on an acceptable format.
- One structure doesn’t fit all – cannot design this with one entity in mind.
- January meeting will feature another discussion on basic points of all the controls? – Dec 2009 is just coming up with examples – Keith is still in the NERC standards format
- Maybe everything can be considered low.
- If just “low” then significantly broadening what security is applied to – Keith is shoehorning the standards into an example control – may need to look at how the federal government works under NIST with FSMA – you get a system of controls that are auditable
- The subgroup is tailoring statements to the current standards in response to NERC requirements for phrasing – yes, spending a lot of time trying to shoe horn it together – if that is not the way to go then let us know before we have created the wrong example.
- My understanding based on discussions with NERC staff –is that unless that statement that auditor is looking at is in a standard with an “Requirement” and been approved as a requirement, it cannot be audited – approval is a process question rather than content – cannot simply just borrow from NIST and run with it.
- Interested in finding out if we can offer it as an example
- Should this group make a formal request through Dave Taylor and Gerry Adamski to Standards Committee to ask for approval for the approach? If we ask now we maybe able to get an answer in 4-6 weeks assuming they do not consider it a change to the standards process
- Does the group want to pursue that option?

- They can authorize the executive committee to act quickly – get on the December docket of the Standards Committee – suggesting creating one bucket with three levels rather than three separate classes to apply NIST to CIP?
- Next standards committee meeting is in Phoenix in January
- Ask permission to put NIST standards out for review to let us go forward and use them?
- No, not the NIST catalogue but agreement that SDT can establish a controls catalogue – the concept, not a specific list.
- Can we produce a lot of controls from the SDT?
- Yes, asking permission to do so since it is not part of the typical standards process.
- This is much more of a risk management concept.
- Have to get a catalogue that goes through the process
- Suggesting a catalogue drawn from NIST and other sources that is appropriate for our industry then do some applicability mapping with h-m-l impact – vast majority of the list will not apply to any one system.
- Scoping and tailoring – not enthusiastic about taking NIST catalogue as a whole to modify.
- Agree to create our own catalogue – NIST just provides a starting point
- And a one size will not fit all
- We have an example of scoping and tailoring effort – careful not to scope and tailor all of the hard stuff out – the current NIST 853 is much more of a "how" than a "what" list – will need to tailor it to fit and also avoid the detail of how.
- Take this discussion into the group of volunteers identified earlier.
- Question- looking at separate document outside CIP-002 – still has to be FERC approved?
- We still need to determine the form and tools needed.
- Will default to be included in the standard anyway?
- Will need to determine what we are asking the Standards Committee – frame the question
- Why are we asking for permission? Don't standards have appendices? Why not go that route?
- Having a catalogue of controls relative to the level of rating to be applied and make it auditable – it may be an appendix – we don't not have a current model and need the Committee's concurrence in developing those controls.
- Question is do we want flexibility?
- 853 is the guidelines – NERC doesn't allow enforcement of guidelines – Keith is rewriting to make it an enforceable standard – catalogues have not been allowed in standards before so we need an okay from Standards Committee for the new model, whether it is in appendix or not.
- IS99 created a technical what standard – non-binding – but was run through their process – we are proposing something similar
- Still want to know why we can't develop as an appendix and simply appraise the committee for their approval – don't want to be distracted given the limited time – declare what we are doing, let them know, and keep moving.
- We can do this in parallel – move forward and create example and also ask Standards Committee for approval of the approach
- Doesn't matter where we put it – makes the standards more readable to put into appendix
- Agree if allowed under current structure

- We are getting wrapped up in format – what are we asking the Standards Committee? How is the catalogue applied? Give flexibility to the entity or have to apply catalogue?
- Catalogue needs to be developed to be dynamic, flexibility to adjust to changes and new attack vectors we can't anticipate
- That will not be acceptable to FERC, NERC or industry – the commission says only those things adopted through their process and made a mandatory reliability standard are enforceable
- We need to refocus on what needs to be accomplished today and going forward.
- Motion/2nd: Draft 1 should be ready by July 2010 for industry comment as part of workplan, addressing all of 706: Yes=11, No=3, Abstain=1.
- More comfortable offering October – we would have to do something different to get there by July – as much as I would like to say and get there in July, it is not realistic.
- Observation -- October is within the 24-month window.
- If deliver before then, all the better.
- Any in July willing to accept October?
- October may be more realistic – other factors mean we should shot for July – expectation is to show progress.
- When will there be a filing with FERC? That is the date that is valid – best possible date for that would be middle of 2011, maybe the end of 2011 to thrown over to FERC.
- Question: it will take a minimum two rounds of comments and minimum one calendar year after the Draft 1 posting to achieve consensus and go to ballot? Wants something formal that talks about the end game
- Question: in the best opinion of the standard drafting team, it will take four rounds of comments and eighteen months after the Draft 1 posting (July 2010) to achieve consensus and go to ballot? Yea=12; Nay=2; Abstain=0

D. SDT Agreements on Structure and Schedule

1. Strawman drafting team (made up of John, Jackie, Phil and John) – with current subgroups completion today or by Nov. 1? Deliverable - can we test what issues that group will tackle? Agreed.

2. Team of Catalogue of Controls volunteers (Joe Doetzl, Bill Winters, Keith Stouffer, Jon Stanford, Jim Breton, Jay Cribb) – address issue of appendix and approval from Standards Committee and report back in Orlando. Given discussion today – Keith's question of format is no longer relevant. Agreed.

3. In the best opinion of the standard drafting team, it will take four rounds of comments and eighteen months after the Draft 1 posting in July 2010 to achieve consensus and go to ballot. (Yes, 12; No 2, Abstain 0)

V. Guidance on issues and questions for the Straw Drafting Team

The SDT identified and then discussed key open issues:

5. Better identification of reliability functions (BES cyber system identification based on reliability functions) – MetaGroup 1 & 2
6. Better definition of terms used in BES mapping document: control centers/systems, generation systems, etc. – MetaGroup 1
7. Cyber impact analysis alternative approaches and implications – avoid unintended consequences – Group 2
8. Better sense of how the pieces fit together and how an entities will use it – reliability functions, where do they fit and how do you come up with cyber systems that apply – Meta Group 1 & 2

Following lunch, members discussed guidance on issues and questions for the Straw Drafting Team to consider including:

A. Better identification of reliability functions (BES cyber system identification based on reliability functions) – Meta Group 1 & 2

Member Comments:

- More than just operating systems.
- Original scope based on functions.
- Look at the definition in the template – changed during the SDT discussion yesterday.
- It appears more restrictive than what we have now you don't operate with a relay further down the system – is this "operate" in the right context?
- Cyber system which supports or performs?
- Strike "reliably" from this.
- Want it to tie into the reliability standards
- "Direct or indirect impact on the reliable operation of" – drawn from the old but has the key phrases
- We will still need good guidance
- Target of protection is a hard item to define.
- I like what is here because it is more the distributive element.
- But never referenced in the standards.
- Access control for connected systems
- Seems like a useful definition that may need to be moved to guidance
- Does the definition cover all the situations? How would control system be treated in terms of data? This is still missing something – this is an IT-centric definition – most people do not think of a relay as processing data.
- Cyber system can be a single device or several – "a discrete set of one or more" – industry sees an out they will take it – a minor add to clarify
- Should you add administration? – a hub is an administration point –
- I think administration is already encompassed here
- And/or display data? Does it add anything?
- Reliability Functions- need to make sure they are defined

- Get back to a brief description – Varnell's group had a list – use that to create definitions – Varnell and Kinas will work on and get to group by Nov. 1.

B. Better definition of terms used in BES mapping document: control centers/systems, generation systems, etc. – Meta Group 1

Member Comments:

- Better definition of BES subsystems?
- May need to use a different term for control center
- Also items that do not fall into the "control center" category – Jackie, John L. and others – will schedule time in the next week or so

C. Cyber impact analysis alternative approaches and implications – avoid unintended consequences – Meta Group 2

Member Comments:

- Are there medium or low cyber systems within BES subsystems?
- If interconnected with high impact systems, does it matter? Are they not high?
- Depends on how cyber system is structured
- Bigger the cyber system becomes the harder it is to manage the security – have to scope to maximum efficiency
- Look at RTUs independently? They are part of the system – some are higher impact than others – don't have to treat them like a control system
- Do all the pieces that make up the system default to high if any one part is high? If RTU is connected it is connected
- For some RTUs it would not matter if they go away
- This is why you need criteria to determine what is high or low impact on cyber impact side
- Can't make assumptions that those things in an integrated entity are all high – may not be in a non-integrated entity
- Reliability coordinator – everyone feeding the system becomes high
- Define the boundaries of the system – where does one begin and another end

D. How can we get a better sense of how the pieces fit together and how entities will use it? This includes where the reliability functions fit and how you come up with cyber systems that apply – Meta Group 1 and 2

VI. Next Steps and closing

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

The SDT adjourned at 2:45 p.m. on October 22.

Appendix # 1— October 20–22, 2009 Meeting Agenda

NOTE:

1. Agenda times may be adjusted as needed during the meeting
2. Subgroup meetings may not have access to telephones and WebEx

Proposed Meeting Objectives and Outcomes

- Welcome new members and outline SDT leadership transition
- Review FERC Order and Discussion of SDT response and industry comment process
- Review the CIP-002 work plan going forward
- Receive updates on TFE, VSLs, VRFs, and related cyber security efforts
- Receive and discuss reports from CIP-002 subgroups identifying key issues and coordination points
- Convene CIP-002 subgroup meetings
- Review and refine a draft outline for CIP-002
- Receive and discuss subgroup reports and draft CIP-002 language
- Agree on work plan, next steps and assignments

October 20, 2009

8:00 Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry
Roll Call; NERC Antitrust Compliance Guidelines
Review of September 9-10 meeting summary and acceptance
8:20 Review of Meeting Objectives, Agenda and Meeting Guidelines — Bob Jones
8:25 Welcome New Members and Leadership Transition — Jeri Domingo-Brewer and Kevin Perry
8:40 Overview of FERC Order on CIP Version 2 — Scott Mix
8:45 Rapid Response Process — Special Meetings and Electronic Voting — Joe Bucciero
8:50 Review and Discussion of Response to FERC Order and Issues with Implementation Plan
10:15 Next Steps and Plan for mid-November Response Document
10:45 Review of CIP 002 Work plan and CIP 002 Subgroup Process — Stu Langton
11:15 Overview of CIP 002 Strawman Template — Joe Bucciero
11:30 Subgroup Reports to the SDT

1. Reliability Functions Subgroup Report and Key Issues and Draft CIP-002 Language — John Varnell
2. List of BES Subsystems/BES Cyber Systems Subgroup Report Key Issues and Draft CIP 002 Language — Jackie Collett
3. BES Mapping Subgroup Report and Key Issues and Draft CIP 002 Language — John Lim
4. Cyber Analysis Subgroup Report, and Key Issues and Draft CIP 002 Language — Phil Huff
5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP 002 Language — Keith Stouffer

3:25 Proposal for Subgroup Meetings — Jeri Domingo-Brewer and Kevin Perry
3:30 Subgroup Drafting Meetings (may be joint subgroups meetings at various locations)

October 21, 2009

8:00 Subgroup Drafting Meetings (at various locations)
10:30 Welcome and Agenda Review — Jeri Domingo-Brewer
10:35 Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure — Jeri Domingo Brewer, Kevin Perry and Scott Mix
10:50 Update on VSLs/VRFs — Scott Mix
10:55 Update on other related cyber security initiatives — SDT Members
11:00 Subgroup Reports — Plenary Session

1. Reliability Functions Subgroup Report, Key Issues and Draft CIP 002 Language
2. List of BES Subsystems/BES Cyber Systems Subgroup Report, Key Issues and Draft CIP 002 Language
3. BES Mapping Subgroup Report Subgroup Report, Key Issues and Draft CIP 002 Language
4. Cyber Analysis Subgroup Report, Key Issues and Draft CIP 002 Language
5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP 002 Language

1:00 Continue Discussion of Key Issues from Subgroup Reports
3:15 Subgroup Drafting Meetings (may be joint subgroups meetings at various locations)

October 22, 2009

8:00 Subgroup Drafting Meetings (at various locations)
9:30 Welcome and Agenda Review — Jeri Domingo-Brewer
9:35 Review of CIP 002 Strawman and Subgroup Reports — Plenary Session

1. Reliability Functions Subgroup Report- Draft CIP 002 Language, Q & A
2. List of BES Subsystems/BES Cyber Systems Subgroup Report, Draft CIP 002 Language
3. BES Mapping Subgroup Report Subgroup Report, Key Issues and Draft CIP 002 Language
4. Cyber Analysis Subgroup Report, Key Issues and Draft CIP 002 Language
5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP-002 Language

1:15 Key Issues from Subgroup Reports and Drafting Assignments Going Forward
2:30 Review Work Plan

- Next Steps for Subgroups and SDT and the creation of a single CIP 002 text
- Review November Version 3 Response
- Meeting Evaluation

3:00 Adjourn

Appendix # 2 Attendees List

Attending in Person — SDT Members

1.	Rob Antonishen	Ontario Power Generation (Friday)
2.	Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
3.	Jim Breton	ERCOT
4.	Jay S. Cribb	Information Security Analyst, Southern Company Services
5.	Joe Doetzl Manager,	Information Security, Kansas City Pwr. & Light Co.
6.	Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7.	Phillip Huff	Arkansas Electric Coop Corporation
8.	Doug Johnson	Exelon Corporation - Commonwealth Edison
9.	Frank Kim	Ontario Hydro
10.	Rich Kinas	Orlando Utilities Commission
11.	John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
12.	David Norton	Entergy
13.	Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, SPP
14.	Christopher A. Peters	ICF International
15.	Scott Rosenberger	Luminant Energy
16.	David S. Revill	Georgia Transmission Corporation
17.	Kevin Sherlin	Sacramento Municipal Utility District
18.	Keith Stouffer	National Institute of Standards & Technology
19.	John D. Varnell	Technology Director, Tenaska Power Services Co.
20.	William Winters	Arizona Public Service, Inc.
21.	Scott Mix	NERC
22.	Joe Bucciero	NERC/Bucciero Assoc.
23.	Hal Beardall	FSU/FCRC
24.	Robert Jones	FSU/FCRC Consensus Center
25.	Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via WebEx and Phone

26.	Brian McKay	Xcel
27.	Jackie Collett	Manitoba Hydro
28.	Tom Hofstetter	NERC

SDT Members Unable to Attend

29.	Jonathan Stanford	Bonneville Power Administration
30.	Sharon Edwards	Duke Energy

Others Attending in Person

31.	Bill Glynn	Westar Energy
32.	Rick Terrell	Luminant
33.	Chris Wright	Burns and MacDonald Engineering

Others Attending via WebEx and Phone

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

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.

Appendix # 4 Meeting Schedule
October 2008–December 2010

Development of CIP Version 2 and Version 3 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 Version 3 process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white papers assigned.

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 Version 3 white 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)

- CIP-002 Subgroup meetings
- CIP-002 Coordination Team meeting

15. October 20–22, 2009 in Kansas City, MI

- SDT Subgroup drafting meetings — day one
- SDT Plenary Session(s) — day two subgroup reports on CIP-002 requirements
- Review and refine initial draft of CIP-002 single text

October–November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–19, 2009 in Orlando, FL

- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.
- November–December Interim WebEx meeting(s)
- Drafting teams as needed to finalize drafts

- CIP-002 Coordination Team meeting

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

- SDT plenary session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment.

Refinement of CIP-002 and Development of Other CIP Standards
January–December 2010
(12 SDT monthly meetings and subgroup WebEx meetings as needed)

- SDT responds to industry comments on initial and subsequent postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-CIP-009 or its successor) OR
- Ballot CIP-002 while permitting industry to rely on CIP 003-CIP-009 until the full suite of controls (i.e. CIP-003-CIP-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP standards for industry ballot
- NERC Board of Trustees adoption of the full suite of standards
- FERC approves and NERC Implements the full suite of CIP standards

Proposed 2010 Meeting Schedule

January 19–21 — Wednesday–Thursday, Atlanta GA	July 14–15, Wednesday–Thursday
February 17–19 —Thursday–Friday, Austin TX	August 11–12, Wednesday–Thursday
March 9–11 — Tuesday–Thursday, Phoenix, AZ	September 8–9, Wednesday–Thursday
April 14–15 — Wednesday–Thursday, Atlanta GA	Oct. 13–14, Wednesday–Thursday or Oct.12–14
May 12–13 — Wednesday–Thursday, Dallas TX	November 17–18, Wednesday–Thursday
June 9–10 — Wednesday–Thursday, Sacramento CA	December 15–16, Wednesday–Thursday

Appendix #5 CIP-002-4 Template

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (insert dates of posting period).
2. Revised SAR and response to comments posted (insert dates of posting period).
3. Revised SAR and response to comments approved by SC (insert date of approval).
4. SDT appointed on (insert date).
5. First draft of proposed standard posted (insert dates of posting period).
6. Second draft of revised standard posted (insert dates of posting period).
7. Third draft of revised standard posted (insert dates of posting period).

Proposed Action Plan and Description of Current Draft:

This is the initial draft of the proposed standard and is being submitted to the Standards Committee with a request to authorize moving the standard forward to the next stage of the standards process.

Future Development Plan:

Anticipated Actions	**Anticipated Date**
1. Post for 30-day pre-ballot review.	(insert dates)
2. Conduct initial ballot.	(insert dates)
3. Post response to comments on initial ballot.	(insert date)
4. Conduct recirculation ballot.	(insert dates)
5. Submit standard to BOT for adoption.	(insert date)
6. File standard with regulatory authorities.	To be determined.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

1. **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.

2. **BES Cyber System —** A Cyber System which has direct or indirect impact on the reliable operation of the Bulk Electric System.

3. **Target of Cyber Protection (Term may not be necessary) —** of the Target of Protection is (1) a set of BES Cyber Systems, (2) the components supporting their confidentiality, integrity, and availability requirements and (3) any other components needing protection based on their network or physical location within the BES Cyber System operating environment.

4. **Cyber System Confidentiality —**Preserving authorized restrictions on information access and disclosure.

5. **Cyber System Integrity —** Guarding against improper modification or destruction of Cyber System settings, presentation and/or data points. This includes ensuring the non-repudiation and authenticity of data.

6. **Cyber System Availability —** Ensuring timely and reliable access to and use of Cyber Systems.

7. **Generation Subsystem**

8. **Transmission Subsystem**

9. **Control Center**

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

1. **Critical Assets**

2. **Critical Cyber Assets**

3. **Cyber Assets**

Appendix # 5

ROUGH DRAFT TEMPLATE FOR INITIAL CONSIDERATION OF CSO706 SDT

Introduction

Title: Cyber Security — BES Cyber System Identification and Classification

Number: CIP-002-4

Purpose: NERC Standards CIP-002-4 through CIP-xxx-4 provide a cyber security framework for the identification and protection of BES Cyber Systems to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification, classification and documentation of the BES Cyber Systems associated with the BES Systems that support the reliability functions of the Bulk Electric System.

Applicability:

Within the text of Standard CIP-002-4, “Responsible Entity” shall mean:

Reliability Coordinator.

Balancing Authority.

Interchange Authority.

Transmission Service Provider.

Transmission Owner.

Transmission Operator.

Generator Owner.

Generator Operator.

Load Serving Entity.

NERC.

Regional Entity.

Structures, components, equipment and systems of facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission that are determined to be associated with Balance of Plant.

Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

(Proposed) Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Requirements

Determine Functions *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

Text, text, text

Text, text, text

Additional paragraphs.

Map Functions to BES Systems

Determine Classification of BES Systems

Responsible Entities shall apply the following criteria to map the list of BES Subsystems supporting the functions described in R1 to High, Medium and Low BES impact categories as follows:

3.1. High Impact (H)

3.1.1. Any Generation Subsystem whose loss results in a frequency deviation exceeding step A of the regional UFLS as calculated using the BA frequency bias setting. (Note BAL-003-0 R5) *(DHS Tier I)*

3.1.2. Any Generation Subsystem that, if lost or misused, results in an Interconnection Reliability Operating Limit (IROL) violation, as determined by an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.3. Any Generation Subsystem pre-designated, long-term as Reliability “must run” units beyond the local utility area by the Balancing Authority, Reliability Coordinator, or Regional Reliability Assurer. *(Critical Asset Guideline)*

3.1.4. Any Generation Subsystem that has been determined to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Regional Reliability Assurer, for voltage stability beyond the local utility area. *(Critical Asset Guideline)*

3.1.5. Transmission Subsystems that contain switching stations 300 KV or higher with an aggregate rated switched capacity flow of 5000 MW or higher in the Eastern and Western Interconnections, or 200 KV or higher with an aggregate rated switched capacity flow of 3000 MW or higher in other Interconnections, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Regional Reliability Assurer, either for voltage or frequency stability support. *(DHS Tier I)*

3.1.6. Transmission Subsystems that, if lost or misused, will result in an Interconnection Reliability Operating Limit (IROL) violation, as determined by an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.7. Transmission Subsystems that, if lost or compromised, will result in the loss of a Generation Subsystem defined in this subsection 2.1, High Impact Subsystems. *(Critical Asset Guideline)*

3.1.8. Transmission Subsystems identified as essential to meeting Nuclear Plant Interface Requirements as per NUC-001 standard for high impact Nuclear facilities.*(Critical Asset Guideline)*

3.1.9. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in voltage collapse as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.10. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.11. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in complete operational failure of the transmission system or separation or Cascading outages. *(Critical Asset Guideline)*

3.1.12. Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystems on 300 KV and above in the Eastern and Western Interconnections, or 200 KV and above in other Interconnections, that have an Adverse Reliability Impact. *(DHS Tier I)*

3.1.13. BES Subsystems that perform automatic load shedding of 300 MW or more.*(Critical Asset Guideline)*

3.1.14. Control Centers and backup Control Centers defined by the transmission assets they monitor or control with a threshold of 300,000 MW total transmission capability.

3.1.15. Control Centers and backup Control Centers defined by the generation assets they monitor or control with a threshold of 10,000 MW or more of total generation.

3.1.16. Control Centers and backup Control Centers defined by the total load they monitor or control with a threshold of 10,000 MW.

3.1.17. Control Centers and backup Control Centers performing Reliability Coordinator functions. .

3.2. Medium Impact (M)

3.2.1. High is: Any Generation Subsystem whose loss results in a frequency deviation exceeding step A of the regional UFLS as calculated using the BA frequency bias setting. (Note BAL-003-0 R5)

Low is: Any Generation Subsystem whose loss results in a frequency deviation up to .05 Hz as calculated using the BA frequency bias setting. (Note BAL-003-0 R5)

Need **“MEDIUM**”

3.2.2. Blackstart Generation Subsystems that have been included in the regional blackstart capability plan as described in EOP 007. *(DHS Tier I)*

3.2.3. Generation Subsystems which, if lost or misused, result in a System Operating Limit (SOL) violation, as determined by an engineering evaluation or other assessment method as explained in FAC-010 and FAC-011. *(Critical Asset Guideline)*

3.2.4. Any Generation Subsystem that has been determined to be essential to the reliability of the BES through an engineering evaluation or other assessment method, either for voltage stability within the local utility area. *(Critical Asset Guideline)*

3.2.5. Transmission Subsystems with 200 KV or higher with an aggregate switched capacity flow of 2,000 MW or higher in the Eastern and Western Interconnections, or with 100 KV or higher with an aggregate switched capacity flow of 1,000 MW or higher in other Interconnections, that have not been included in Section 2.1 above, that have been determined to be essential to the reliability of the BES through an engineering evaluation or other assessment method, either for voltage or frequency support. *(DHS Tier II)*

3.2.6. Transmission Subsystems comprising the Cranking Paths identified in EOP 005-2 R1.5. Transmission Subsystems that, if lost or misus*ed, results in a System Operating Lim*it (SOL) violation, as determined by an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.2.7. Transmission Subsystems that, if lost or compromised, will result in the loss of a Generation Subsystem defined in this subsection 2.2, Medium Impact Subsystems. *(Critical Asset Guideline)*

3.2.8. Transmission Subsystems identified as essential to meeting Nuclear Plant Interface Requirements as per NUC-001-1 for Medium Impact Nuclear facilities.

3.2.9. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, results in cascading outages that affect areas of the BES system within the local utility area, as determined through an engineering evaluation or other assessment method.

3.2.10. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in voltage going below the under-voltage load-shed points, as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.2.11. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in frequency going below the under-frequency load-shed points, as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.2.12. Special Protection Systems (SPS) or Remedial Action Scheme (RAS) Subsystems on less than 300 KV in the Eastern and Western Interconnections, or on less than 200 KV in other Interconnections that have an Adverse Reliability Impact. *)*

3.2.13. Control Centers and backup Control Centers defined by the transmission assets they monitor or control with a threshold of 100,000 MW or higher total transmission capability, not already included in Section 2.1 above.

3.2.14. Control Centers and backup Control Centers defined by the generation assets they monitor or control with a threshold of 5,000 MW or more of total generation, not already included in Section 2.1 above.

3.2.15. Control Centers and backup Control Centers defined by the total load they monitor or control with a threshold of 5,000 MW, not already included in Section 2.1 above.

3.3. Low Impact (L)
Everything else??

Determine BES Cyber Systems that support the BES Systems

(R5a) Determine Classification of BES Cyber Systems

The Responsible Entity shall identify and categorize its BES Cyber Systems using the following steps for each BES Cyber System:

- **BES Subsystem Mapping —** Identify all BES Subsystems through which the BES Cyber System supports or has the potential to impact one or more Reliability Functions.

- **Reliability Function Assessment —** Assess the potential function impact the BES Cyber System has on each of the associated BES Subsystems given the loss of Confidentiality, Integrity, or Availability within the BES Cyber System. Assign one of the following function impact categories for each BES Subsystem the BES Cyber System supports.
  - **High —** Severe degradation or loss of control of the BES Subsystem to an extent and duration that the Responsible Entity cannot perform one or more of its Reliability Functions.
  - **Medium —** Significant degradation or loss of control of the BES Subsystem to an extent or duration that the Responsible Entity can perform its Reliability Function, but the effectiveness is reduced.
  - **Low —** Degradation or loss of control of the BES Subsystem to an extent or duration that the Responsible Entity can perform its Reliability Function, but the effectiveness is noticeably reduced.

R5b. The Responsible Entity shall identify its BES Cyber Systems and determine the potential impact on the BES based on the loss, misuse or compromise of the BES Cyber System (according to [BES Mapping Table]). *(** Need to develop the reliability impact definition and the impact criteria definition for High, Med, and Low. Aggregation of BES subsystems and BES cyber systems versus the impact criteria needs to be defined. **)*

Merge Classification of BES Systems and BES Cyber Systems

Provisional Impact Categorization — Assign a provisional impact category to each BES Subsystem associated with the BES Cyber System using the following look-up table as a relation of both the potential function impact and BES impact mapping.

BES Impact Function Impact	High	Medium	Low
High	**High**	**Medium**	**Low**
Medium	**Medium**	**Medium**	**Low**
Low	**Low**	**Low**	**Low**

Final Categorization — Assign the resultant impact categorization of the BES Cyber System as the maximum provisional impact category from its associated reliability functions. Once the Responsible Entity has determined a provisional impact of High, then they need not perform additional impact analysis.

Document resultant Classification

Approval resultant list

Measures

M1. Text

Compliance

Compliance Monitoring Process

Compliance Enforcement Authority

- Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- ERO for Regional Entity.
- Third-party monitor without vested interest in the outcome for NERC.

Compliance Monitoring Period and Reset Time Frame

Not applicable.

Data Retention

- The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

Compliance Monitoring and Assessment Processes

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

Additional Compliance Information

Text

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL

Regional Variances

None.

Associated Documents

VERSION HISTORY

Version	Date	Action	Change Tracking
4.000	10/20/2009	Initial draft of Version 4 Use of new format standard template	