NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Cyber Security Order 706 SDT — Project 2008-06

September 9, 2009 | 8 a.m. – 5 p.m. PST
September 10, 2009 | 8 a.m. – 4:30 p.m. PST
Folsom, CA

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

Joe Bucciero, Bucciero Consulting, LLC

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT 706 September 9-10, 2009 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT 706 SEPTEMBER 9-10, 2009 MEETING

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer welcomed the members to Folsom California and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On day two the SDT accepted the August 20-21 meeting summary without comment or objection.

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.

Mr. Langton reviewed the CIP 002 work plan between August and December 2009 which the SDT adopted at its meeting in Vancouver, setting up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the Chair and Vice Chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. Mr. Langton reminded the five subgroups that they have about two more months to finish their work of developing proposed draft language for the new CIP-002 Version 4 standard, and the full SDT will then work to finalize the new draft CIP-002-4 standard for posting to the industry for comment in December 2009. He noted by the conclusion of the October 2009 SDT meeting, the goal is to have a single draft CIP 002-4 that can be debated and refined in November and adopted in December.

Jackie Collett & Phil Huff & Jeri Domingo Brewer provided the SDT with a review of the August 25th Industry Webinar on the concept paper. The Webinar participation was estimated to be over 650 participants with more than 800 registered.

Jeri Domingo Brewer and Scott Mix jointly presented an update on the TFE process. The Chair noted that at the conclusion of the August meeting, she had agreed to follow up with the Standards Committee regarding the SDT support for addressing TFE issues as an urgent matter. She indicated she will be presenting these to the Committee soon. Scott Mix noted that on the Rules of Procedure side the NERC 2nd draft posting is in comment process now and the Comment period has been extended to Sept 11.

Scott Mix provided a brief update on Version 2 VRF and VSLs noting that the pre-ballot comment period will close September 10 with a 10-day ballot period immediately following the comment period. A recirculation ballot is a high probability, since there is likely to be a comment from an entity voting no. He noted that in the future, the SDT 706 will be responsible for Version 3 VSLs and VRFs and will need to accomplish this in its 2010 workplan.

The following related industry initiatives update was provided:

- In the past week an industry meeting was convened to update the DOE Control Systems Security Roadmap which was initially developed 3 years ago.
- There is a NIST working group, Cyber Security Coordination Task Group (CSCTG), that is focused on smart grid cyber security issues that has been holding weekly conference calls, and its current face-to-face meeting is being held at the same time as this SDT meeting. The CSCTG is in the process of defining cyber security requirements for the various application and functional interfaces that exist among the various computer systems that are utilized by utilities. They are organizing their work to address FERC's four priority policy areas for the smart grid (Demand Response, Electric Storage, Electric Vehicles, and Wide Area Situational Awareness), plus two additional areas of AMI/AMR and Distribution Grid Management. They will be consolidating their inputs into a Smart Grid Framework and Roadmap document, as well as providing a NIST Interagency Report (NISTIR) on Cyber Security. For each interface, they will propose security controls. The NIST site has documents posted, and they should be released shortly for industry comment and feedback.
- The NERC Planning Committee has established a small working group and is soliciting applications for membership in the working group that will focus on cyber security of smart grid components.

Scott Mix presented an overview of the industry comments received on the draft concept paper, noting that 49 comments were submitted by the deadline (Sept. 4) with three additional sets being received following the deadline for a total of 52 comments consisting of over 140 pages. Scott suggested the comments were "all over the map." Few of the commenters, if any, expressed general agreement with the approach. Many struggled to understand of the process and either didn't understand or didn't agree with process.

The SDT reviewed the draft concept paper comments and discussed what the SDT's vision for success is in putting these pieces together from the feedback and comments. Below are the elements of the vision of success suggested by SDT members:

- Standards that will assure the reliability of the BES.
- Multiple groups of people running through the process with same inputs/requirements will reach the same conclusion.
- The end result passes the "smell test"- engineering analysis would agree with the results.
- Industry recognition that reliability functions are important and understanding why protection is needed and beneficial. Focus on reliability functions can demonstrate reliability of BES.
- A clear enforceable standard that doesn't create an unnecessary hardship on entities.
- Get requirements on paper that are simple for entities to follow but may be complex in their development.

The SDT identified the following themes in the industry comments:

- Clarify the SDT philosophy and approach in terms of the degree of flexibility vs. prescription provided in the standards.
- Seek simplification in the final standard but engage in complex hard issues in getting there. Achieve some simplification: workable, clear and doable.
- Engineering analysis needs to support any thresholds. SDT should do this as part of setting the standard.

The SDT identified the following issues from industry comments:

- Complexity.
- CIP-002 Not Yet Tested.
- Augment existing CIP requirements with elements of SDT concept paper.
- Should the SDT take on CIP 003-009 sooner than 2010?
- Value of a walk through example for the SDT and industry.
- Role of Adequate Level of Reliability (ALR) in Concept.
- Pilot the Concept Paper approach.
- CIP 002 as Cornerstone.
- Concern about scope.
- Thresholds and Engineering Analysis needed to support standard.

Scott Mix brought a request from Mike Assante at NERC to the SDT. He asked whether the SDT could confirm that the existing exemption for non-routable protocols will not be carried forward into Version 3? Or in the alternative, can the SDT confirm it will be considering the removal of the non-routable exception for future systems and any modifications to current systems? He noted that the impact of a device is not a function of communication protocols-which are better covered in the list of requirements on how to secure the device.

In light of the SDT discussion, Mr. Mix brought the following statement to the SDT for its consideration, and it indicated a 3.6 out of 4 point consensus scale indicating support for the following statement:

Concerning the elimination of the blanket exemption for non-routable protocol connected serial devices, as is being considered for inclusion in the scope of the CIP Cyber Security Standards, assume the following:

1. The removal of the exemption will not be applicable to the existing approved Version 1 or Version 2, but will be considered in future versions of the standards.
2. The specific security requirements for serially connected devices will be contained in the “catalog of security requirements” (currently CIP-003 through CIP-009), properly accounting for the threat and vulnerability components to the risk to the device.
3. An appropriate implementation plan will need to be adopted recognizing the number of devices brought into scope by this change

The SDT will recommend that the blanket exemption not continue into Version 3, such that communications to a device will not be a consideration for the impact to reliability of the

device. Mr. Mix agreed to provide Mr. Assante with a sense of the team's position on this issue.

Jackie Collett, SDT member, agreed to conduct an informal concept walk-through the proposed conceptual approach to CIP 002 for the SDT with an example that starts with identification of the functions. She started by noting that the SDT needs to develop a vision of what this is going to look like comparing it to designing a vehicle when you are not sure if it's a bike, truck, car, or van.

Using restoration as a function, she suggested that a list of generating units, transformers, station busses, transmission lines, and associated loads for balancing as the BES subsystems supporting this function.

Members identified the following key questions in the course of the Functional Walk-Through:

- One of the industry's questions was how much flexibility should be given to the entities in determining the applicable BES subsystems. If no flexibility in identification and categorizing is given, then you don't need to put a methodology in the standard.
- Do the supporting pieces together create the BES subsystem?
- Will there be consistent outcomes going through the restoration functional analysis first or going through the cyber analysis first?
- If same generator does both restoration and other reliability functions, how to address aggregation in terms of its categorization?
- How to deal with multiple reliability functions from multiple entities?
- Do you need reliability functions mentioned in the standards? This might be part of the development of the standards but would reduce complexity if functions not included in the standards.
- Should there be a "none" or "no impact" category for the functions included in the BES list?
- For which subsystems do we need to do BES mapping?
- Is redundancy protection aimed at failure vs. compromise?
- Should we apply controls at cyber system level, or a methodology to a device level?
- What do we apply controls to: system or components of the system?
- How can we address interconnected systems and systems we are dependent?
- What about interconnectivity with other systems that are ranked differently?
- What is the SDT philosophy and approach- i.e. degree of flexibility vs. prescriptive, guide or impose? How to go about this? What is our strategy?
- Who can determine impact to the reliability of BES? Owner of asset has to even if they have no way to. Is this the right way to go. Who has wide enough view and capable of doing this?

On day two, Joe Doetzl reminded the SDT that the concept paper offered entities the choice of an alternative approach that started with the cyber systems and map those. The concept suggested that the different starting points should result in the same ending point. The

complexity comes from the BES mapping and reliability functions and different levels of impacts on each of those systems. The question is whether if you start with the cyber system it will be a simpler approach to cyber security than starting with the reliability functions.

Members identified the following key questions in the course of the Cyber Analysis Walk-Through:

- What would a responsible entity do in determining what should be in the scope to protect?
- On cyber side, if the cyber is deemed impactful does it inherit the impact level of the function supporting the BES assets? Is anything not impactful not in scope?
- For the assessment of functions or on asset supporting reliability function, do you need an intermediate step?
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those?
- Can the assets mapping be capable of translation to a systems approach?
- Any way to diminish the impact of the audit process on low impact sites?
- What does it mean for a BES cyber system to support a reliability function? Is it info for situational awareness, control to generation, etc?
- Are there systems we unequivocally expect to be protected? Basic SCADA systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out.

SDT members discussed what was learned through the walk through of the functional and cyber approaches including:

- The two walk-throughs indicated there is a similarity in complexity in both approaches.
- The issue is how do we eliminate complexity regardless of which side we start the analysis. For example in the cyber approach the complexity is contained in Step 3 whereas in the functional approach it appeared in Step 2.
- Neither is more complex that the other as it will depend on the environment and context. Large number of BES and small number assets may start on cyber side. Small number BES and lots of cyber may want to start on the BES functional side. Neither is wrong.

On the first day of the meeting, the SDT heard and discussed reports from each of the subgroups. The subgroups then met on the second day to review and respond to the comments and suggestions of the SDT.

On the first day Rich Kinas reported, on behalf of John Varnell, on the Reliability Functions Subgroup's work. He noted the subgroup has redistributed its members into other subgroups. The subgroup will continue to try to put more definitions around what was meant by different functions including a brief paragraph on each and what is meant for benefit of and guidance to the other subgroups.

Jackie Collett noted the BES Subsystems subgroup had no further meetings since the August Charlotte meeting. She noted that Jim Case and Matt Greek from the NERC Operating Committee are now participating on the subgroup. On day two, she reported that the subgroup still needs to put time and effort into defining what these BES subsystems are and move into drafting requirements.

John Lim noted the BES Mapping Subgroup met to continue its work in developing the BES Mapping draft markup and was joined by members from the Functions subgroup. Two major issues the subgroup is dealing with include: how do we validate an engineering study? Approval by regional reliability assurer? TFE type process? Need to look at this more. Note that no entities currently are performing the role of reliability assurer. Also, what is meant by "Misuse"- need to describe this term.
John Lim reported following the BES Mapping Subgroup's meeting on day two. The Subgroup is drafting a set of requirements for High, Medium, and Low. There are still questions on how to handle industry studies. In terms of generation subsystems, he noted they are using terms that are not very well defined (e.g., subsystems in generating stations). The terminology they are using must be precise and consistent and coordinated with Jackie Collett's subgroup.

Phil Huff delivered the initial Cyber Analysis Subgroup report noting his confusion about how the subgroup should go forward. BES impact categorization as the black box is a flawed assumption. The subgroup could reduce some of the complexity in the process. We assumed each function mapped would have an impact categorization so we could combine through a "look-up table." On day two, Mr. Huff noted that his subgroup would huddle when the SDT breaks. He noted that there may not be as much confusion as was stated yesterday. Impact criteria that are involved in John Lim's one-to-one mapping will be considered. The subteam needs to develop a strategy on the cyber analysis side.

Keith Stouffer presented the Definition and Selection of Controls subgroup's report. He noted that during the Charlotte meeting the subgroup developed and presented an example based on access control. We pulled together into one location the access control referenced in many places. Keith mentioned that the format is new and the subgroup doesn't know if this is acceptable. Need to nail down as soon as possible what is an acceptable format. The Subgroup on day two noted they will seek to nail the format decision down with NERC. Joe Bucciero will send latest work in progress of the Subgroup to all group leaders.

The SDT agreed that a brief statement should be drafted for publication in NERC's newsletter. Gerry Freese agreed to draft the summary. The Chair reviewed with the SDT the schedule for the next couple of meetings, reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP 002 which we can refine in November and approve for posting in December. She thanked the members for their hard work together and in the Subgroups and encouraged them to continue working to make headway on each of their charges. Members completed an onsite meeting evaluation form.

The SDT adjourned at 3:45 p.m. on September 10.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT 706 SEPTEMBER 9-10, 2009 MEETING SUMMARY

I. INTRODUCTIONS, AGENDA AND SDT WORK PLAN REVIEW

The Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). The SDT adopted the August 10-11 meeting summary without comment or objection on Thursday morning.

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.

Mr. Langton reviewed the CIP 002 work plan between August and December, 2009 which the SDT adopted at its meeting in Vancouver, setting up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the Chair and Vice Chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. He noted the five subgroups have about two months to finish their work of developing the CIP 002 draft to be finalized by the SDT in November and December, and released for posting and industry comment in December 2009. He noted by the conclusion of the October 2009 SDT meeting, the goal is to have a single draft CIP 002 that can be debated and refined in November and adopted in December.

Member Comments on SDT Workplan

- Due to increased workload in terms of response to CIP-002 industry comments and the development of CIP-003-009 requirements in 2010, the SDT will be convening 3-day meetings
- The SDT will continue to use phone and telephone conference calls to enhance effectiveness.
- As an alternative, NERC staff brought up the possibility of meeting 1 to 2 weeks at a time to improve schedule effectiveness.
- The current proposed game plan- is to set SDT meetings using 3-day schedules with a back-up strategy of spending a 1-week chunk somewhere, if needed.
- At first blush this appears shocking. However, when you factor in the day traveling/to and from it might not be more onerous than the current meeting schedule.
- The hosts for the remaining 2009 SDT meetings are checking to see if they can add a 3rd day to each of their meetings.

Jackie Collett & Phil Huff & Jeri Domingo Brewer provided the SDT with a review of the recent Webinar (held on August 25) on the working concept paper that was posted to promote information exchange with the industry. The Webinar participation was estimated at over 650 with more than 800 registered. The SDT leaders indicated the session went well and Joe Bucciero agreed to get the Webinar summary notes out to the Team. Questions were raised surrounding the security controls which underlined the importance of work ahead. There were process questions of what version would be implemented when? NERC staff didn't jump in to answer questions as this was designed as an SDT Webinar. Those questions were referred to NERC for responses.

Member comments on the Webinar Presentation

- In terms of questions dealing with process and NERC standards, communications with the industry is needed. We need to do a better job of telling the industry what they should be doing. There is significant confusion currently.
- The Chair proposed and the SDT agreed to do another Webinar in the December time frame with the Subgroup leaders participating. NERC will need to flesh out with the industry the process area questions.

II. UPDATES

A. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure

Jeri Domingo Brewer and Scott Mix jointly presented an update on the TFE process. The Chair noted that at the conclusion of the August meeting, she had agreed to follow up with the Standards Committee regarding the SDT support for addressing TFE issues as an urgent matter. She indicated she will be presenting these to the Committee soon. The Chair noted that Kevin Perry is prepared to move forward with an urgent action SAR that was reviewed and discussed at the August SDT meeting and is looking for a proxy to submit.

Scott Mix noted that on the Rules of Procedure side the NERC 2nd draft posting is in comment process now and the Comment period has been extended to Sept 11. They have received 5 sets of comments which NERC staff is reviewing.

In the context of interim guidance issues for those entities in compliant phase, regions are in process of figuring out how to handle these. NERC is trying to get the interim process running ASAP while the formality of approving the final process takes place.

Member Comments on SDT

- Has a decision been made on the matrix for the SAR? In August Mr. Perry noted it was "vetted" it with regional group representatives on the CCWG group and the chair of the Version 1 CIP.
- Where do we go to get guidance for entities coming up on an audit and the status of TFEs? The interim guidance document on NERC website--which NERC drafted and regions have

agreed to. Updated interim guidance is under development to make interim more consistent with final if approved.

- What if a region has no facility for accepting TFEs? Rely on your own legal council.
- Last posting of TOP is one we should expect to be implemented. Section A- by September 17, 2009. The assumption is that the implementation proposed is best we know right now.
- In July 2008 there were 13 requirements compliance by July 2009, there were 41 requirements. The regions are hanging in the wind on this. One entity represented on the SDT is 5 weeks from a NERC audit. Members are confused. Need to make things easier.
- The MPCC in discussing the ROP has pointed out FERC hasn't approved version 2 yet. Version 1 of standard only? Will we have to change again?

B. Update on VSLs/VRFs

Scott Mix provided a brief update on Version 2 VRF and VSLs noting that the pre-ballot comment period will close September 10 with a 10-day ballot period following with recirculation a high probability if there is a single comment from an entity voting no. In the future, the SDT 706 will be responsible for Version 3 VSLs and VRFs and will need to accomplish this in its 2010 workplan.

C. Update on other related cyber security initiatives- *SDT Members*

Keith Stouffer noted that in the past week a meeting was convened of over 100 experts in La Jolla, California to update DOE Control Systems Security Roadmap which was initially developed 3 years ago. They addressed activities and initiatives over 3 years, e.g. smart grid and SDT 706. Energetics provided facilitators to manage a number of break-outs. They are under contract to produce an update to the road map in the next few months. The website is: http://www.PublicIERoadmap.com

There is a NIST working Control Center ETG focused on smart grid issues that is meeting today and tomorrow. They are collecting interface security requirements and are looking at FERC's four areas of focus. They will be consolidating inputs into 1 document. For each interface, they will propose security controls. The NIST site has documents posted.

The NERC Planning Committee has established a small working group and is soliciting applications for membership in the working group that will focus on cyber security of smart grid components. They understand they need enough of a cyber security perspective on the working group and the Planning and Operating committees don't typically have that perspective. They are looking at the electric grid reliability impacts of smart grid(s). You can't do smart grid without high speed communication. A fundamental tenet of this is requiring good cyber security.

III. REVIEW OF INDUSTRY COMMENTS ON THE CONCEPT PAPER

A. Overview of Industry Comments

Scott Mix presented an overview of the industry comments noting that 49 comments were submitted by the deadline with three additional sets following the deadline for a total of 52 comments consisting of over 140 pages. He suggested the comments were "all over the map." Few of the commenters, if any, expressed general agreement with the approach. Many struggled to understand of the process and either didn't understand or didn't agree with process. Some took exception to the breadth and scope of the concept suggesting it may exceed the authority of 215 Fed Power Act. Responses to Question 5 are typical of the diversity of perspectives: some believed 3 levels is the right number, others suggested higher and lower numbers, including 2 levels of critical and non critical and others suggested leaving it as it is currently.

B. Overview of Member Comments

1. Overall Themes of SDT Reflections on Industry Comments

- Clarify the SDT philosophy and approach in terms of the degree of flexibility vs. prescription provided in the standards. Trying to get away from the current wide latitude and flexibility. How much less latitude? How much room for judgment? If give latitude. If entity can provide an alternative approach through an analysis, this will increase the complexity of the standard if you have to outline what will be an acceptable analysis.
- Seek simplification in the final standard but engage in complex hard issues in getting there. Achieve some simplification: workable, clear and doable. Engineering analysis needs to support any thresholds. SDT should do this as part of setting the standard.

2. Vision of SDT Success

The SDT reviewed the comments and discussed what the SDT's vision for success in putting these pieces together to do? Below are elements of the vision of success suggested by members:

- Standards that will assure the reliability of the BES.
- Multiple groups of people running through the process with same inputs/requirements will reach the same conclusion.
- The end result passes the "smell test"- engineering analysis would agree with the results.
- Industry recognition that reliability functions are important and understanding why protection is needed and beneficial. Focus on reliability functions can demonstrate reliability of BES.
- A clear enforceable standard that doesn't create an unnecessary hardship on entities.
- Get requirements on paper that are simple for entities to follow but may be complex in their development.

3. SDT Identification of Issues from Industry Comments on Concept Paper

   a. Complexity. Is the concept too complex as presented?

b. CIP OO2 Not Yet Tested. Haven't run with existing CIP 002 long enough- consider staying with it longer?
c. Augment existing CIP with elements of SDT concept paper. Recommend to take valuable elements of new approach to augment legacy CIP 002-009 framework.
d. Should the SDT take on CIP 003-009 sooner? Is there another way to deal with "dodgers"- can we take another look at what we need to deal with CIP 003-009. E.g. grading high medium and low. Significant concurrence with moving in direction with identifying controls. Should we look at how to improve 3-9 and then back to 002? Hunt down dodgers.
e. Value of a walk through example for the SDT and industry. Help the SDT and the industry to walk through process CIP 002 start to finish with some mythical power plant, control center or sub station. How to go from defining system, to applying controls to assets. "Systems" is the new concept and how to help the industry make this leap. Walk through as a team. We would better tell our story and let people understand it. Haven't stepped all the way through this process.
f. Role of ALR in Concept. What was missed in responses is that the concept of ALR is not going to appear in the CIP 002 standard. It is a framework for deriving the functions. The functions will be included, not the ALR. They only served as a guide for drafting team to derive functions that are relevant. They served as principles for getting at the scope for 002. If you ignore principle 6, the other 5 principles are in line with Federal Power Act at a high level. ALR defines adequate levels of reliability.
g. Pilot the Concept Paper approach. May need a pilot for the concept similar to how this is done in the nuclear side to test how it works in practice.
h. CIP 002 as Cornerstone. The SDT made a strategic decision to develop CIP 002 as the cornerstone. It is ugly and difficult work. We can't drop this, we have to finish it even though it is hard.
i. Concern about Scope. Industry concern is that no one knows how big this will be—there is a "paranoia about scope". Concern also of the possible loss of invested effort (time and $$). Is there a way of taking what has been done and map it to the CIP Version 1 and 2 to see what happens to the critical cyber assets. Industry is asking how much more will we have to do than what we do now. If the under Verion 1 and 2 represents 10% of critical assets. Will I have to spend 10 times as much under version 3?
j. Thresholds and Engineering Analysis to Support. If this drafting team puts out hard threshold numbers it need solid engineering analysis behind it.

4. Member Review of Industry Input on Concept Paper

a. Wednesday Member Discussion Notes
   - Some suggested we didn't provide enough detail for them to respond, even though this was presented as a concept paper. A few entities didn't understand the concept.

- Overall, it appears many didn't understand what the rationale was for changing the existing process changes believing the existing didn't have a chance to prove itself.
- Lots of discussions among drafting team over last 6 months. Going forward, we need to lay out more clearly why we are moving in this direction. Set forth why this sea-change is being proposed in identifying and categorizing?
- Industry may be upset because we are perceived as a moving away from compliance and trying to address security. What we do currently is compliance oriented.
- If the SDT and industry do this right, both security and compliance can be achieved. This is a new way of looking at security that is trying to do just that.
- My take is different. I believe we should take the critique of concept complexity seriously. It is mentioned 40 times in the comments. Confusing is mentioned 31 times and complicated is referenced 12 times.
- SDT has to be aware of and trying to not making this more complicated than is needed.
- Some are suggesting we should not start with ALR- which is suggested to be too broad a starting point. Instead consider starting with Federal Power Act definition of reliability and build on basic approach.
- The concern with ALR may be directed at principle 6. The other 5 are more in support of the Federal Power Act reliability definition. Enough generation to serve load.
- Written by Operation and Planning Committees- wrote this on reliability. Is this service reliability vs. bulk electric reliability.
- Yes it is a complex process- we started with 3 levels. Created a complex process that overloaded the front-end analysis. Entities not sure of how to implement. Hard #s would make it easier and simpler. Higher impact- easy to understand. Push back is that engineering analysis may find that is quite right. Are we painting the house with a small brush in order to keep the paint off?
- We may have gotten so few comments because of the complexity and the other things out there.
- Compliance vs. security discussions- compliance is overwhelmed with evidence they must provide. Reluctant to introduce additional documentation/evidence requirements.
- Should we focus on 003-009 where we have problems and come back to 002? FERC order 706 had many issues with 003-009.
- If we provided some relief and flexibility in that area? Easier to expand later.
- There is a concern with putting out 002 in a vacuum- CIP 003-009 most concerned with. What do I have to do? We need to post a sample with 002.
- In the current paperwork drill and compliance we are forgetting security. Is there a possibility of a quick hit on something helpful in 003-009? If this is another paperwork nightmare, could get voted down. How are we going to get

there from here? Don't have a vision for success that we can articulate to the industry.

- Is the concept too far reaching on CIP 002 aspect? One comment suggested it is too complex and should run with existing CIP 002 long enough to judge its effectiveness.
- Another way to deal with "dodgers"- can we take another look at what we need to deal with CIP 003-009. E.g. grading high medium and low. Significant concurrence with moving in direction with identifying control.
- Should we look at how to improve 3-9 and then come back to 002? Hunt down dodgers.
- We need to help industry to walk through process CIP 002 from start to finish with some mythical power plant, control center or sub station. How will this go from defining the system to applying controls to assets?
- "Systems"- how to make this leap. Walk through as a team. We would better tell our story and let people understand it. Haven't stepped all the way through this process.
- Paper work drill. Can't repeat with new standards. Seeing future audits of standards being more operational vs. paper work. If we are going to get this security- test operations to see if secure. Operational audit only way to do this in a hands on way. Don't know how this will happen. Need to think about. Pie in the sky? E.g. "Penetration test"
- Audits will do more of this in the future.
- Agree with today's SDT comments. We still have a focus on paperwork for audits.
- The industry is hesitant to walk away from the compliance investment.
- Recommend valuable elements of new approach that can augment the legacy framework of CIP 002-009.
- Should ALR be the beginning point? Does ALR need to be removed?
- ALRs- if we ignore principle 6 right now, the other 5 principles are in line with the Federal Power Act at a high level. Back up protection schemes were presented in Phoenix. Where in the system are these systems required? How to determine this? ALR defines adequate levels of reliability. Maybe we should have 2 levels. High impact and low impact? Low impact- difference with Version 1 or 2- got to do something more than the current model requires. E.g. issues with password managing, patching. Different levels of e.g. patch management. Comes into requirements section is where that belongs.
- Support for using the current CIP as basis and augmenting with new things.
- What was missed in the industry responses is that the concept of ALR is not going to appear in the standard. It is a framework for deriving the functions. The functions will be included not the ALR. It serves as a guide for the drafting team to derive functions that are relevant. They are just principles for getting at scope.

- If we stick with a multi level approach in 003-009, we will need to know what we are devising requirements for. OO2 does this. Put out an example. Categorizing system. Medium or high system show applying security controls. Show that not every single asset will have a requirement. Will be more complicated as a compliance exercise.
- The regions seemed to be suggesting that the concept appears good but there is a suggestion that what may be needed now is a pilot. Similar things done on nuclear side to see how it works. We don't know how it is working but we invested lots of $$. Audits- going on now. Think right now of a case study or pilot.
- Critical assets, non-critical assets and de-minimus assets?
- The concept seeks to provide strategic decision- CIP 002 is the cornerstone, albeit, ugly and difficult for the SDT. We can't drop it and say this is too hard yet.
- What is desperately needed is what is low is? That's why getting this. Everything will be protected. Give both high and low.
- There is a concern that no one knows how big this will be—i.e. a "paranoia about scope". Concern of loss of invested effort (time and $$).
- SDT should consider a way of taking what has been done, providing a mapping of what has been done- a critical asset- critical cyber asset- show that mapping and what happens if you apply the concept paper. Critical assets and critical cyber assets- question is the middle ground. Industry wants to know how much more will we have to do than what we do now?
- If I currently devote 10% to facilitating critical assets, will I have to spend 10 times as much under the concept?
- Routable vs. non-routable- trying to be a physical security standard while calling itself a cyber security standard. Can we address this? CIP 10- physical security. Big disconnect- something important but not protecting.

b. Thursday Member Discussion Notes

At the beginning of the discussion on Thursday of the Industry input, the facilitators summarized several key questions raised in Wednesday's discussion including:

- Are there systems we unequivocally expect to be protected? Basic SCADA systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out
- On the cyber side, if the cyber is impactful, then it inherits the impact level/ function of the BES assets it is supporting. Anything not impactful is not in scope. This could be one way to simplify the process.
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those? In end multiple levels of cyber systems impact on function.

- Define what it means for a BES cyber system to support a reliability function. Is it info for situational awareness, control to generation, etc?

Member Comments

- Clarification and simplicity to make this a more manageable change process.
- Didn't hear industry rejection of fundamental assumptions and model.
- Threshold model approach?
- Upon reflection there might not as much confusion as we initially thought.
- Our team need to develop more on the cyber analysis side.
- We haven't decided whether there will be a one-to-one mapping. Can't promise that yet. Lots of overlapping functions. Level of functions we have is higher in the criteria than the functions we have from Subgroup 1.
- Subgroup 1 functions- BES assets list- covered all functions rather than a 1-1 mapping.
- Supporting documentation will be critical to communicate to the industry how we got there.
- Is there existing mapping of any generation sub system? Building on work already done and look for thoroughness.
- Matrix- started in middle of concept. 2 sides of matrix. Decoupled approach then use matrix to combine. Laid out some general thresholds. Supporter of thresholds.
- Generation subsystems
- The 19 criteria John Lim's group identified covering high/medium and low- may not be enough. Raw megawatt output, Constraint mitigation, radial vs. non radial etc.
- The SDT should consider applying watermarking on that generation.
- Based on around 10 generation criteria
- Then Cyber impact- may not have hard number- describing impact of cyber system to the BES subsystem generator. Impact is same whether big or small. Combination of cyber and BES impact accommodated in the final result. Feed into CIP 003-009. Below was is an example to illustrate the concept that Scott Mix shared with the SDT:

	High	*Med.*	*Low*	*Null*
BES impact e.g.	<2001	<1001	<400	Less than 400

	High	*Med.*	*Low*	*Null*
Cyber impact:				

- Is this per unit or per plant? One row for per plant and another row per unit? Need to determine this as well. Per unit on cyber side and per plant on BES side. E.g. a plant wide scope of control?
- Degree of simplification- detailed work. Should this team take this one on?. Assume it should be done. Punt to somebody else?
- Don't know its been done to this level. Is that a scope of work for a cyber security person. If we don't do it, no one else will.

- Subgroup understanding. Making marriage of two impact assessments. Way to move forward to define the cyber impact criteria. What does it mean for BES cyber system to support the reliability functions. May not have H/M/L levels.
- Proposal on evaluation of cyber system- proposing a H/M/L on its impact on the function? Most functions map to BES subsystem.
- Analyze the Impact to the system.
- Impacts to the reliability function are de-coupled. This is not how it impacts the BES systems.
- We may be counting the impact twice on each side.
- In the federal context, the White House defined criteria for defining cyber system impact on a business function level. Marrying top-down and bottoms-up approach. Painful process to begin with. Interpreting top down approach. Has become easier to develop what controls apply.
- E.g., boiler flame control system- what cyber- reliability function of generation. Not counting twice. Make sure clear on what a BES cyber system is. Define it on a functional level—i.e. what it means for cyber system to support at reliability function.
- What happens if the cyber system isn't there. Only defined cyber system as supporting a reliability function.
- High =loss or compromise of confidentiality, integrity and accessibility. Medium= there are effects, not expected to effect.
- The size of a generator does not play into cyber analysis.
- The cyber system inherits the rating of the BES asset. Like to consider a cyber analysis as binary. Cyber systems not associated with "big iron."
- It is an issue of scope of control.
- Now that you know the function- e.g. EMS what cyber systems are and they inherit EMS. E.g. historian functions, offline logging system probably low.
- Assets essential to perform that scope of control are inherited. Bottom out at low.
- Point out that here are the filters that help place these in the buckets.
- The cyber impact doesn't trump the BES impacts.
- We are assuming inputs of categorized reliability functions. We can define them for reliability. Don't have a list of cyber functions.
- The SDT needs to get the requirements down. Take this opportunity to know what we need to do in writing.
- Numbers- is there a threshold number assumed that can be applied? Risk based methodology (guideline 27). "Bright line"- categorization of what constitutes a BES.
- Are we coordinating with other regional entities? SDT represents all the regions. NPCC doing this? Bring to everyone else? NPCC aversion to "bright lines" (A 10 as methodology for id critical assets for CIPs standards)
- NPCC- only region that has used the NERC definition of bulk power. Issued a performance-based methodology to determine what is bulk power with backup studies. Guideline 27 is a regional guideline.

- We may need something talks about constraints- relieve IRLs or SOLs. VAR support and voltage support. We will need a number of yardsticks to determine criticality.
- Control center- simpler map back to transmission and generation? Numbers of links and lines? Relationship to elements underlying that.
- Are there other reliability standards under draft- similar process determining applicability to BES elements. Rationalize with them and make it the same? E.g. disturbance reporting standard.
- NERC attempted to do that in Version 1 but fell short. Criteria for disturbance reporting is an early warning gray area. (warning track).
- Determination of bright lines. Focus on cyber security side. Are we in danger of going down rabbit holes?

C. Exemption for Non-Routable Protocols

Scott Mix brought a request from Mike Assante at NERC to the SDT. He asked whether the SDT could confirm that existing exemption for non-routable protocols will not be carried forward into Version 3? Or in the alternative, can the SDT confirm it will be considering the removal of the non-routable exception for future systems and any modifications to current systems? He noted that the impact of a device not a function of communication protocols- better covered in list of requirements on how to secure the device.

Member Comments on the Request

- Non-routable protocols may be as susceptible to attack as routable, e.g. electronic security perimeters are not feasible, patch management and other things, incidence management. Attach those requirements to other cyber devices.
- What was the logic behind non-routable exception? Why did we do this?
- Primarily around electronic protection- firewall kind of device. Because we cant do ESPS, ended as a blanket exemption.
- Wouldn't have a problem supporting this. However there is no implementation plan under CIP Version 1 yet. Can we allot sufficient time for compliance?
- Newly identified critical assets- Version 1 / 2 may take from 6 to 24 months to implement.
- Under version 1- physical security on nuclear sites? This won't happen. Can we accomplish this within the time limits?
- Intent question= CIP 2 version 1- exclusions were deliberate- initial starting point. Couldn't deal with the serial devices issues and left it out at that time. Too much for industry to start with and swallow. Has anything changed?
- Need to address effective security for those devices. Some measure of physical security.
- Implementation plan- version 2- different implementation plan.

- Michael Assante's request- appropriate for Team to respond with a position- our task is to improve the overall cyber security stance of the industry. We will consider what is appropriate for modern and legacy serial devices and risk/vulnerabilities associated with this.
- Many took prudent measures to provide some level of security for those devices serial in nature.
- The SDT will need to do thorough analysis of the implications before we take a stand on this. We shouldn't address now unless we fix everything else.
- assuming that exclusion is on the table to be lifted in version 3, assuming that we appropriately address requirements for serial devices. Ok with assumptions.
- Assuming you mean the future CIP standards instead of system the Team is considering the need for exceptions to the standards.
- This question has nothing to do with version 3 of the standard.
- Grandfathering the non routable as it is
- He is asking if regardless of version 3 of standards, are we going to do something to stop people from changing or replacing systems.
- There is a difference between exemption and exception. Are we talking about an exemption? We need clarification of what he's asking.

Draft Statement

In light of the discussion above, later in the afternoon Scott Mix brought the following statement to the SDT for its consideration:

> Concerning the elimination of the blanket exemption for non-routable protocol connected serial devices as being considered for inclusion in the scope of the CIP Cyber Security Standards:
>
> Assuming the following:
>
> 1. The removal of the exemption will <u>not</u> be applicable to the ~~next version of the standards (Version 3), but not to the~~ existing approved Version 1 or Version 2), <u>but will be considered in future versions of the standards.</u>
> 2. The specific security requirements for serially connected devices will be contained in the "catalog of security requirements" (currently CIP-003 through CIP-009), properly accounting for the threat and vulnerability components to the risk to the device.
> 3. An appropriate implementation plan will need to be adopted recognizing that the number of devices brought into scope by this change
>
> The SDT will recommend that the blanket exemption not continue into Version 3, such that communications to a device will not be a consideration for the impact to reliability of the device.

	4=acceptable	*3= minor reservations*	*2=major reservations*	*1= not acceptable*
SDT Rating	**7**	**9**	**1**	**1**

Comments before the Rating

- Concerns with stating it will be removed. JDB
- "will be applicable.
- Assumptions imply this is the position of the team as a whole. Discussed exceptions but hadn't concluded that Version 3 will need exceptions.
- We haven't made that conclusion.
- The SDT does not intend to include a similar clause in CIP 002 differentiating between routable and non-routable protocols.
- We haven't walked up and touched the elephant.
- Impatient-consider this reasonable- we will consider it in the future. No objection.
- The issue of non-routable protocols will be addressed in…. implying this in the 002 concept. Target of protection may lead you to communications that are routable.
- The SDT hasn't discussed this. Needs to be vetted.
- We don't know yet whether you keep them in or take them out.
- Yes we will look at this in version 3.
- If version 3 is targeted at something else, want to make sure that any decisions incorporate sufficient time for implementation.
- Keep it simple. Eliminating it? Not for Version 1 or 2.
- This is an apple and oranges issue. "Critical cyber asset" What we are doing has nothing to do with this. Different ball game. No idea how connectivity will play into categorization.
- This doesn't belong in 002 but in the individual controls.
- Appropriate to respond- that impact is not related to communications connectivity.
- We don't know how we are handling connectivity.
- If Mike Assante wants the SDT to consider this further, he should provide a statement in advance of a meeting so the SDT can understand the intent. E.g. was it to prevent routable communications from being ripped out of service and replaced with non routable to not have critical cyber assets to apply security controls?
- Interpretation cannot modify standards.
- Scott Mix will provide Mr. Assante with a sense of the team's position on this issue.

IV. SDT CONCEPT PAPER WALK THROUGH

A. Walking CIP 002 Through an Example- Restoration Functional

Jackie Collett, SDT member, agreed to conduct an informal concept walk-through the proposed conceptual approach to CIP 002 with the SDT with an example that starts with identification of the functions. She started by noting that the SDT needs to develop a vision of

what this is going to look like comparing it to designing a vehicle when you are not sure if it's a bike, truck, car, van.

Using restoration as a function, she suggested that a list of generating units, transformers, station busses, transmission lines, and associated loads for balancing as the BES subsystems supporting this function.

Member Walk-Through Key Questions

- One of the industry's question was how much flexibility will we give the entities in determining the applicable BES subsystems. If no flexibility in identification and categorizing, then you don't need to put a methodology in standard.
- Do the supporting pieces together create the BES subsystem?
- How much flexibility should there be for the entity? Should there be pre-determined criteria?
- Will there be consistent outcomes going through the restoration functional analysis first or going through the cyber analysis first.
- If same generator does both restoration and other reliability functions, how to address aggregation in terms of its categorization?
- How to deal with multiple reliability functions from multiple entities?
- Do you need reliability functions mentioned in the standards? This might be part of the development of the standards but would reduce complexity if functions not included in the standards.
- Should there be a "none" under this function as part of the BES list?
- What are the subsystems we need to do BES mapping for?
- Is redundancy protection aimed at failure vs. compromise?
- Should we apply controls at cyber system level, or a methodology to a device level?
- What do we apply controls to: system or components of the system?
- How can we address interconnected systems and systems we are dependent?
- What about interconnectivity with other systems that are ranked differently?
- What is the SDT philosophy and approach- i.e. degree of flexibility vs. prescriptive, guide or impose? How to go about this? What is our strategy?
- Who can determine impact to the reliability of BES? Owner of asset has to even if they have no way to. Is this the right way to go. Who has wide enough view and capable of doing this?

Member Discussion Comments

- One of the industry's question was how much flexibility will we give the entities in determining the applicable BES subsystems.
- There will be an EOP- works for restoration? Assume for this example that there isn't an EOP- assets work together
- Do we expect every registered entity to perform restoration?
- Do these supporting pieces together create the BES subsystem?
- Today it is asset based. Generation as critical asset without transmission being critical?

- List of BES subsystem stuff.
- Do we apply the criteria to BES subsystems or parts?
- Before we apply, do we need to make sure the list of assets is impactful to the BES? If not it shouldn't go into categorization system.
- How much flexibility should there be for the entity? Should there be pre-determined criteria?
- Entities should apply criteria to BES sub system to determine whether the subsystem is in scope.
- Is it the low threshold?
- When we started work of categorization, we assumed that the things have some impact, high, medium and rest is low. Should we define low? And everything else is out of scope.
- 1 for generation and 1 for transmission.
- High impact- part of regional restoration plan.
- Apply the criteria to generation and this is medium.
- High impact- transmission sub system- comprising 2 or more paths.
- When we reference the regional blackstart plan we should acknowledge the potential for gaming.
- Assume that this vehicle has to drive properly. How will this work?
- Is the level a binary evaluation? Are you are either part of it or you are not? You are high or low?
- This may not be in keeping with the way we are trying to look at this as a whole.
- Should transmission and generation be in the same class?
- Compliance- generation operator/owner and transmission owner/operator.
- Consistent outcomes? Go thru restoration functional analysis and have one categorization and through another analysis and come up with another. Does this create extra work? Some pieces will likely do another function. Joe Doetzl agreed to do a walk through the other side of the optional concept approach.
- Once you hit high- you are high.
- Aggregation issue :If same generator does restoration and other functions. Supports multiple reliability functions does that change its categorization?
- Will this introduce too much subjectivity and complexity
- Flexibility=complexity. How much flexibility will entities be provided? If no flexibility in identification and categorizing, then you don't need to put a methodology in standard. Would greatly simplify by giving marching orders.
- Multiple functions from multiple entities. E.g. situational awareness for 2 entities, and control and operations for another. Substation monitored by control center. Another entity with control center does control from station.
- This is part of agreement and oversight. BES subsystem side and the same issue will be there for cyber systems.
- What are the cyber systems associated with "big iron" system that is ranked high? Associated with the big iron system and its function.

- BES subsystem- just supporting the big iron stuff ranked as a high.
- What are the cyber systems associated with big iron?
- Impact categorization. Developing criteria- mentioning the function and the BES subsystem. All within the criteria. Do you need reliability functions mentioned in the standards?
- This would be part of the development of the standards- would reduce complexity if functions not in standards.
- From a compliance point of view this might be an issue. The reason for first list is so you can know they are all categorized.
- BES sub system based on reliability function with no H/M/L criteria- where would that place.
- Will we define the low threshold or will this be done by the development of the list of BES subsystems that are in scope.
- Lows are now a "catch hold." Criteria for high and medium are specified and if it is not in those then it is placed in a low category functioning as a default category.
- If we introduce a "none" category, then we need a low impact. Could be a "none" under this function. Would the "none" be part of the BES list?
- We developed a list of functions and BES mapping. Are all essential functions represented by one of the BES mapping criteria? Do we need to start with functions? Make sure all essential functions are represented in the mapping.
- Need a way to check that all are included in a bucket.
- You would have a restoration criteria? Yes. Ensure all functions are captured in the mapping criteria.
- From impact categorization, it is easier to think of generation, transmission etc. vs. functions.
- If we do the BES mapping of functions into the criteria, we need to make sure we have covered all the functions at appropriate level in the criteria.
- How does BES subsystem fit into this?
- Is the entity going to determine what sub systems are or will a table be provided.
- What they would like to see, if you are a generator and you perform this function and above this many megawatts, you are a high.
- Start with the asset not the function. Risk is you will miss systems supporting functions that are not part of the asset.
- Mapping BES subsystems to reliability functions. Current assumption- impact criteria would reference some finite set of BES subsystems.
- Stayed away from generating stations. Stating the impact criteria in terms of BES sub systems? Yes.
- Would have minimal set of subsystems- if you have these kinds, performing these functions, have to be evaluated as a generation subsystem.
- We need to define the reliability functions in terms the industry can understand.
- Reliability functions- every asset involved in situational awareness or balancing load and generation.

- What are the subsystems we need to do BES mapping for?
- How do we work in those doing engineering studies now to do ranking of assets? Has the universe been covered in these reliability functions?
- Jeff Gillen ATC noted that the industry has done a lot of work already. There may be an industry problem if ALR and existing planning standards aren't tied to this. Things should be done with existing methodologies if possible. Planning criteria for category A, B, C etc. Category C event is looking from a common mode failure of a cyber attack.
- Industry understands the current methodology. Consider building on it. Analysis looking at cascading.
- This is one of the inputs for coming up with the list by the Mapping Group.
- We have identified a major stumbling block on identification of BES sub systems. However an alternative appears available for building on what exists today.
- Categorizing cyber systems. It is not until Step 5 of methodology and finally talk about cyber systems.
- BES subsystems and categorized and now identify BES cyber systems. Look at BES cyber systems (SCADA, control system). Look at all of BES systems/
- Assume we identify BES cyber systems that support reliability functions of the BES.
- Identified- to the asset which supports the functions. Generating stations- remote RTU, SCADA, master, blackstart, local in plant controls. How do you then apply the controls. Do an analysis of your cyber systems.
- Which subgroup is looking at defining or describing a cyber system? Here's its cyber system- in house plant controls. Apply appropriate/adequate controls.
- If compromised cyber system (integrity, confidentiality, reliability) how would it impact reliability of BES.
- None not low. Cyber standard. If no cyber stuff, it doesn't apply.
- Functional impact analysis. What would it mean to impact restoration? E.g. metering in the station provides situational awareness, but not highly required. If start/stop controls rely on meters. Meters then part of a start/stop system.
- What is the basis of being low?
- General criteria h/m/l. If it is compromised can you continue to perform your function.
- Blackstart relying on remote communication. Regional restoration plan is a way-documented.
- Final step is to combine the assessment to the look up table. How many systems are you protecting for?
- Redundancy is another complexity issue. Identify the primary preferred blackstart paths. Three primary blackstart cranking paths. Protect all the same. Need to protect any of them. What are you protecting for.
- Redundancy is protection for failure not for compromise. Issue of redundancy- dealt with at identification of BES subsystem.
- How should we deal with redundant cyber sub-systems? Should redundant equal same?

- Planners might argue that redundancy has an impact- might not solve all but most.
- Standards today- generators- engineered the utility grid so that nothing is critical?
- On the cyber side- even if you have four redundant systems, if one gets the virus, all may have it depending on connectivity. Have to plan that way.
- Issue is if you don't protect those 2 systems, all could be compromised through cyber means. Often don't know when compromised.
- Set of cyber systems, applied an impact category on it. How do we apply our controls? Local control system in a generating plant.
- Can we have a meaningful discussion of controls?
- Is a cyber system a DCS? Targeted protection. What is a DCS? 1000s of cyber systems or one system with an impact rating.
- How much flexibility should there be for the entity?
- If you apply single category to that is is clear what you need to do, but it takes long time to get done.
- Multiple levels of granularity- don't know what to do and we risk spending all your time figuring out what to do.
- Simplicity vs. complexity. You need the analysis so to apply security controls.
- Currently defining down to a CCA level. It may be the DCS and a subcomponent brings along the baggage of the DCS.
- Define target of protection- several controls will be common across
- Risk management- and address TFE.
- How does this work within a FISMA framework. DCS at Hoover. Microprocessor devices. Expectation from NIST?
- The understanding in NIST is that you analyze the security engineering process on your system. Go through and determine if it is a moderate impact system. Here are security controls I need to comply to the system.
- In order meet this requirement, you need to meet this access control by applying to central access control management.
- E.g. measurement of flow on spillway.
- "Scoping and Tailoring"- is the NIST term. Scope it out. Provide rationale as to why not. Oversight on process? As long as you can argue and win with your IGs. Puts lots on the auditor for quality types of assessment.
- Should we apply controls at cyber system level, or a methodology to a device level?
- As a team should we think about a different path?
- You may need to go down to the equipment level not stopping at systems.
- Go further down from DCS system level to the component level to effectively apply the controls.
- Scoping the target of protection- you need to tailor it? Do we further subdivide? TOP-DCS.
- DCS: 1 or 2 primary processors/computers, operating work stations, engineering work stations, HMI, slave components, data acquisition components, interfaces to business system.

- TOP universe of systems you need to protect.
- What do we apply controls to: system or components of the system? It will depends on the control. No cut and dry answer.
- Risk management framework uses compensating controls. You can meet the intent of control on component by doing other things.
- How have the federal agencies implemented 800-53 to field devices. Apply to individual level?
- Use a 'Control inheritance' concept and use the "tailoring and scoping" exercise. Come up with Compensating controls. All of this is documented in the security plan appropriately. Acceptance of risk is not allowed by FERC. How can we develop a hybrid approach?
- Puzzle pieces are fitting together better through this discussion.
- One-to-one mapping between reliability functions and BES subsystem may not be possible.
- How can we address interconnected systems and systems we are dependent?
- Identified cyber system focusing on and components making up system.
- What we haven't done is defining target of protection.
- Determine interconnected cyber systems that support the BES functions. E.g. DCS- in the model is control equipment- interconnected cyber system? It depends. On how you connect workstations to them. Network design is important to note.
- Once BES system is in scope. We need to determine how the system resides in the architecture and what are the components within system.
- Does ranking of components consider the factor of functions or connectivity?
- Connectivity defines controls or high/medium/low.
- Distributed control systems- plant controls- generator.
- What about interconnectivity with other systems that are ranked differently?
- Typical DCS may not communicate off campus.
- Assumption that identified TOP- done the methodology- interconnected systems inherit the rankings. TOP – assumes BES cyber system is a single element? Drawings suggest already part of system.
- E.g. Conflicker worm- hooked up to internet- through dumb workstations.
- Difference in understanding and perception- of a system from an operations side or a data side. This is the old model- look forward to new model.
- Target of protection model value- what is my realm of influence if compromised?
- Access control is key to security- network, operating, application and facility layer.
- TOP- e.g. email server. High impact. TOP control center- Rules and what applies- need to distinguish- unique target areas. TOP- showed how when you got to BES cyber system- interconnected nature- won't know where to place your control. Email server- negligent case of putting on same network at DCS switch.
- Inheritance of levels into collateral systems- apply same analysis on these systems as we apply to other. Impact on mission- each cyber system impact/support mission- calling that reliability functions.

- TOP- apply the same analysis to these. Some may rely on email systems more than others in terms of impact – fulfillment of mission. We learned they needed redundancy of email systems.
- When federal organizations categorize their systems- they consider the potential impact to missions, assets or individuals. Consider potential impact to other organizations they are connected with.
- The lowest level needs some level of security.
- The reason systems outside of BES cyber system. In TOP collateral- could be compromised and could compromise. Required for operation of BES cyber system. Impact on BES cyber- leads to categorization. This is not because of their inherent effect on reliability function itself.
- Concept paper does good job of explaining in TOP- have to secure because they could be a entry point for compromise.
- Identifying Cyber system and TOP. Does TOP just scope how you hare defined your system. Helps you determine what you need to protection.
- Collateral systems- if there are no requirements- won't make it into a standard.
- TOP- 3 in paper- prototypes- 3 environments we built them for. Shouldn't be hard fast rules of what should be where. Auditor should look for this.
- Higher level steps in the process. Concerned about value added.

Concluding Comments- Functional Approach Walk-Through

- What we defined the bicycle- reaction on the whole step through
- First steps- some were confused about the value adding of the step. Think about eliminating and moving on to important steps.
- Last step- TOP passionate about.
- Any candidates for eliminating or simplifying?
- 1st part is more conceptual and complicated. Latter part is more grounded.
- 1st part is new where applying security controls is not new.
- This can be can be simplified. The complexity may be more evident in the development process, where the final standard may be simpler to present.
- TOP- Subgroup 4. Will come out in the controls section. Put a boundary of some sort around the system and protect it.
- We are moving away from perimeter protection and move towards influence control.
- There remain fundamental gaps between 2 groups approaches.
- Need to address how much flexibility. How will we present this to industry? We need a simpler recipe.
- This remains Confusing. How do we expect the industry to understand this? Too complex and confusing. Industry won't buy. Congress will ask whether you have secured the system and they feel that the industry not being forthcoming in their comments regarding money.
- We should seek to integrate the pieces or simplify the entire model.

- It this predicated on the maturity of industry? Cyber security-maturity models are still 3-5 years out.
- What is the SDT's understanding of the maturity level of the industry in terms of security? Don't have a good feel for where the industry is in thinking and acting on this.
- Simplifying CIP 002 is going to be imperative.
- We should develop a strawman set of thresholds to test drive among us. Today's exercise helped show implications of the concept and we learned a lot. What do we need to do to move the level of maturity in the industry along. More proscriptive may be justified today. Not traditional reliability.
- What is the SDT philosophy and approach- i.e. degree of flexibility vs. prescriptive, guide or impose. How to go about this? What is our strategy.
- Give the industry some flexibility to make some of their own decisions? Trying to get away from the current scheme? How much less latitude. If we offer room for judgment, we will give latitude.
- Are we blending the two? Hard limits, low water mark. Entity could provide alternative through analysis. Implication is the complication in the standards?
- Low water mark- opt in and add to it- increase their compliance footprint.
- Engineering analysis needs to support any thresholds. Do this as part of setting the standard.
- Seek simplification with how to go about this. Achieve some simplification: workable, clear and doable.
- Readiness assessment- was eliminated – had some excellence of operation.
- Compliance audit- immature organization. Some organization do betters than others.
- Audit- prohibited from going and making kinds of recommendations.
- Review existing and trying to develop more performance based standards?
- Should lay out what you need to do vs. how to do it.
- The problem with CIP 002 may be 003-009
- What would happen if left risk methodology in CIP 002. If fixed 003-009 would every one say.
- Response to industry from the drafting team should convey that we have read comments and we are considering things.
- De we make time to try another model? Model is in the concept paper. It identifies for us things we could keep in mind.
- Who can determine impact to the reliability of BES? Owner of asset has to even if they have no way to. Is this the right way to go. Who has wide enough view and is willing to do this.
- Consider the Abeline paradox regarding the impact of group think.

B. Walk-through- Cyber Approach

On day two, Joe Doetzl reminded the SDT that the concept paper offered entities the choice of an alternative approach that started with the cyber systems and map those. The concept suggested that the different starting points should result in the same ending point. The

complexity comes from the BES mapping and reliability functions and different levels of impacts on each of those systems. The question is whether if you start with the cyber system it will be a simpler approach to cyber security than starting with the reliability functions.

Member Walk-Through Key Questions

- What would a responsible entity do in determining what should be in the scope to protect?
- On cyber side, if the cyber is deemed impactful does it inherit the impact level/ of the function supporting the BES assets? Is anything not impactful not in scope?
- For the assessment of functions or on asset supporting reliability function, do you need an intermediate step?
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those?
- Can the assets mapping be capable of translation to a systems approach?
- Any way to diminish the impact of the audit process on low impact sites?
- What does it mean for a BES cyber system to support a reliability function. Is it info for situational awareness, control to generation, etc?
- Are there systems we unequivocally expect to be protected? Basic SCADA systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out.

Step 1- Inventory Cyber systems Involved

At the entity level, for this example, assume a complete inventory of cyber systems. A list of cyber systems you may find in a typical utility could include:

- Customer info and billing systems
- Financial info systems
- HR system
- EMS system
- Blackburn generating unit (2) and associated control system. (black start system)
- Load Master Units 1-8-single control system for all units
- Distribution automation system.
- Protection system (relays)

Member Comments

- 1000s of systems that won't fall into list. Monitoring, desktop systems, Corporate info security vs. power. Guidance will be needed to industry help understand what should be included on list. For example, what is the process for ruling out the HR system?
- Assume multiple security officers and do this more than once.
- What would a responsible entity do in determining what should be in the scope to protect? If start with cyber system need all cyber systems in inventory.
- Assume separate corp. systems from control? Manageable group of systems.

- At some point make an analysis that it isn't connected with reliability- impact categorization?

Step 2- BES Mapping for These Systems

Joe Doetzl suggested the key question here was do these systems directly support the reliability of BES?

- Customer info and billing systems NO
- Financial info systems NO
- HR system NO
- EMS system YES
- Blackburn generating unit (2) and associated control system. (black start system) YES
- Great Big Coal Burner Units 1-8-single control system for all units (big enough) YES (based on functions-
- Distribution automation system. ?? Depends- YES
- Protective system (relays) YES
- Smart grid (maybe, depends)

Member Comments

- AMI unit?
- Will distribution be covered? No, Federal Power Act- excludes distribution.

Step 3. Perform Impact assessment to determine what level of impact cyber systems on reliability of the BES.

BES Mapping Subgroup will be helping to address this through their mapping. In the alternative, any connection must put control on. We should give industry flexibility in choosing which controls will get them to baseline security for their assets. Ask the question, what is your worst-case scenario if this cyber system goes bad do the assessment.

Member Comment

- Assessment of functions or on asset supporting reliability function. Need an intermediate step.
- EMS will be easy case to tie to BES.
- In our BES mapping document we provide a methodology for saying H/M/L. Maybe there is a way to translate John Lim's work to get to H/M/L buckets.
- Complexity lies in that mapping.
- Alternative is if there is any level of impact- that dictates what you need to do.
- When do you look at inputs to the system to determine whether in scope? TOP approach?
- Step 4- look at this in examining security of each system. If our EMS system has a connection into HR system, brings it back in. Running on same server you are back in.

- Need to add a lot of detail to bring this together. We haven't done what this implies.

Step 4. Apply controls appropriate to the level of impact each cyber system needs to have.

Member Comment

- How will the level of impact be done?
- Should we do away with the impact of the cyber system itself? If the cyber system falls into category because it falls within one of the BES functions- That system automatically falls in the high. Have to make assessment of what is the effect of the cyber system if compromised, on the BES subsystem and make a determination then of what category would fall in.
- Confidentiality, integrity and availability of the system lost- resulting a categorization at H/M/L. Assessing the EMS system and go to functions mapped to- go to table being developed by John Lim vs. a matrix. It will have the BES cyber system and will help determine what the impacts would be using the impact "look up tables." Alternatively, no flexibility, this is set in advance.
- Choose in standard development process. Does your cyber system support reliability? If yes, apply baseline set of controls.
- SM: how do you do #3.
- Look at impact- generator- load support and system stability, ability to provide megawatt, loss of mw in short period of time. In restoration it doesn't. Depends on which impact you are looking at.
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those? In end multiple levels of cyber systems impact on function.
- Categorization of cyber assets- if impactful, all or nothing, similar to CIP today.
- By starting with ALR, have we caused confusion? This e.g.- pp 17, entities may choose to use an alternative approach. Alternative method- straw dog.
- While the industry is not necessarily that familiar with the ALR, start with systems that are essential to the tenets in the ALR- e.g. to restoration. All the systems that support these things. Cut down the confusion about inventory.
- Mapping that John Lim has done has been on assets not systems. Maybe able to translate it to a systems approach. Customized to provide tool for systems not assets.
- Don't think this departs from 3 levels of impacts. Binary on cyber analysis side. Still have mapping to subsystems with H/M/L. You just look at whether it supports.
- 2 levels of impact analysis. BES asset and cyber impact analysis on assets/functions. Simplifying either one into binary step. Simplifying both would be drastic and less palatable.
- Complexity of impact assessments is large. In the end you have appropriate controls, are we better served than by picking a set of controls. Put on everything. Don't know yet in terms of controls.
- MITRE study that Jason Marshall talked about CIP 3-9 didn't meet the NIST moderate baseline.
- Would get industry documenting controls.

- Are we taking steps backwards? Not taking account levels. Check everything and add controls. Trying to do too much on cyber stuff and not worrying about BES first.

C. Lessons learned from the Walk-Throughs

SDT members discussed what was learned through the walk through of the functional and cyber approaches. Below are a summary of their comments:

- The two walk-throughs indicated there is a similarity in complexity in both approaches.
- The issue is how do we eliminate complexity not on which side we start the analysis. For example in the cyber approach the complexity is contained in Step 3 whereas in the functional approach it appeared in Step 2.
- Neither is more complex that the other as it will depend on the environment and context. Large number of BES and small number assets may start on cyber side. Small number BES and lots of cyber may want to start on the BES functional side. Neither is wrong.
- The categorization process for government systems is not cut-and-dried with ambiguity in it. Organization provides enough evidence to bosses that this is a correct categorization. Need something more cut and dried. Possibly thresholds. More consistent and cut and dry.
- Rather than dwell on 1 method that identifies 5K vs. 50K then big issues, we should be getting the same generally from both.
- Confusion about this in terms of what it would mean in changes. Simplification comments came. Simplify by saying you have to do a lot to everything. Flexibility in what we do to them. The latter is what we have today. Here is everything you have to do.
- If you simplify step 3- broad brush- not in the paper. Option #1- broad swath doing something to lots of things, you figure out what you want to do.
- The SDT should put in a lot of work in reducing complexity of the process. Make it clearer on where we are heading. On cyber side, is the cyber impactful, then it inherits the impact level/ function it supporting of the BES assets. Anything not impactful is not in scope. Could be one way to simplify the process.
- Eliminating cyber h/m/l.
- This is simpler than yesterday- fewer steps. Took less time. In support of simplifying the process. 2 impact assessment one for assets and one for systems.
- One is binary and the other is 3 levels.
- Is the team in support to simplifying the approach?
- Reducing the assessment to one that is binary vs. 3 levels to simplify?
- Assumed the BES subsystem impacts. Had the same complexity. Still have to look at BES subsystems.
- Performing impact on reliability functions.
- Define what it means for a BES cyber system to support a reliability function. Is it info for situational awareness, control to generation, etc?

- What does success look like for us at a Team? Do we get consistent and good answer going on both approaches. Part of problem in evaluating 2 different approaches. When everyone applies, do we get the same answer and does it provide BES reliability.
- Success=
  1. multiple groups of people running through the process with same inputs and requirements reach the same conclusion.
  2. End result passes the smell test- engineering analysis would agree with the results.
- Having too much is not as dangerous as not enough of the right thing.
- Success= a clear enforceable standard that doesn't create an unnecessary hardship on entities.
- Reliability functions important- protecting something and knowing why this is beneficial.
- E.g. generators- size, time and connectivity are considered. Focus on reliability functions can demonstrate reliability of BES.
- What will be the ultimate impact on entity?
- Complexity- current standard- complexity at the entity. Take complexity into the standard, doesn't go away.
- Are there systems we unequivocally expect to be protected. Basic scada systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out
- SM: hide complexity behind the scenes in supporting documents and have some thresholds that are not arbitrary and capricious. Some threshold number a basis in power system engineering. Generation transmission and control centers.
- Simple- multiple step. Spend time figuring out the buckets.
- 4 Interconnections- transmissions characteristics within and between. 19 # in JLs document. Publish paper that justifies thresholds.
- Sacrilege to the planning and operating group.
- Simplifying what the expectations and obligations of what industry have to do.
- Rod: H- depends on what controls you are talking about. No explanation of what is happening downstream. Make decisions to place assets in too high a category. Costing a fortune for daily maintenance.
- More heavily weighted toward a high impact because of implications in implementing controls.
- Set of criteria- you have some high, more in medium and a heck a lot in low category. More rational and justifiable methodology.
- What will be the bucket sizes 10% less high, 40% less medium, 50% low. If we that many high assets something is wrong with the criteria.
- Yes we could come up with some numbers. New CIP 005 controls. 1000 RTUs and downstream devices with user management on them.
- Come up with classification levels and set of controls. Look at how applies to field distributed devices, substations, etc. This is where the push back comes from.
- Supports when you look at control system. what are the components of that system? Focus on impact and the function of device. This helps to set up boundaries.

- Impact analysis of cyber system: determine what is it's span of control? A relay on a single line is a small span of control. How much control with a single cyber system.
- Does low not mean zero? Baseline everywhere.
- Address cyber systems that have no impacts.
- Do we have a good handle on what is industry security posture? Significant number of entities avoiding audit world. Is there another way- certain auditable levels with high. Any way to diminish the impact of the audit process on low impact sites?
- ERCOT implemented for all systems- technical security framework. Figured out 1 set of rules. Biggest headache is documentation of compliance especially doesn't contribute to security baselines. Things in the "high" bucket auditable compliance. In reliability business, key to reliability is change control. Integration testing etc. Concerned about federal model and the volumes of documentation that may be required.
- How should we treat aggregated BES systems- 30 generators. In the categorization we should give consideration to aggregate assets with their own impact assessment performed vs. based on asset.
- Bringing up concept Jackie Collett brought up yesterday on a subsystem basis. Meeting multiple criteria at medium. Does it bump up from medium to high?
- When compound a bunch of functions- have to look whether it magnifies the impact? Is there any consideration for some kinds of redundancy?
- On the cyber side- span of control- from one plant to lots of plants. Do you factor in redundancy? Master control center and remote units. Are each as important as the Master?
- Control Center- doing something for one generation station. Cyber high. 1 low BES vs. 30 low BES.
- Span of control of asset that has overview over multiple.
- Didn't expect that system would get down to that granular level.
- Evaluating device as a control system. Cyber system has a common impact to multiple BES system- analyzed under a span of control.
- If I have connectivity to systems what is the scope of influence. Address a field system and a breaker on in terms of scope of influence? Span of control? Can you impact a high enough level e.g. of mw.?
- If on the same network- can I impact multiple units? Other considerations that are not covered.
- Work through these issues on a case study basis.
- BES subsystems- stretched thin when you deal with these sorts of things, e.g. high pressure oil lift system.
- We need flexibility so that standards lead you to the right conclusion.
- Area impacts. The control center is where the impact is assessed.

V. SUBGROUP REPORTS TO THE SDT

On the first day the SDT heard and discussed reports from each of the subgroups. The subgroups then met on second day to review and respond to the comments and suggestions of the SDT.

A. Reliability Functions Subgroup Reports, *Rich Kinas*

1. Day One Report

On the first day Rich Kinas reported, on behalf of John Varnell, on the Reliability Subgroup's work since the last meeting covering the following points:

- Defining Functions Critical to reliable operation of the BES
- 9 functions initially but after making some changes up to #5 there are probably only 8 functions
- "Balancing Load part of controlling frequency"? Leave it stand alone to make more sense to the industry
- Not planning to go further than 3 levels down.
- Tried to identify the functional subsystems that would have to be addressed.
- At which step of the process, do entities fall out of the flow? Consider within each of the 4 subgroups
- The BES Mapping subgroup (John Lim et al) is setting up thresholds.
- The SDT needs to be thinking of the subsystems and pieces of sub systems that will perform these functions.
- Address and protect everything in subsystem whether you own it or not.

Member Comments

- The Subgroup got feedback from John Lim's Mapping Subgroup.
- At the highest level- look at ALR and refine what this means in the world? All the current reliability standards are direct descendants of the ALR.
- Burning question- what do we do with this list? Input to scope the BES subsystems and cyber systems. Or are we defining impact? Where do we go from this list?
- The Subgroup wrestled with this. The sooner we define impact, the better. Do we do this before addressing subsystems?
- Impact criteria table-of several pages long- Will industry want this? Understand this?
- Create a list of questions that each entity had to answer, result would determine whether they meet the criteria or not? And at what level?
- At what level do you ask those questions. For every function? Take it to level that is feasible by December. Cant go to 3rd level.
- Look at individual functions vs. very generic criteria
- A question at top under dynamic response-
- BES Mapping subgroup – not going to go towards an increased granularity of functions. Define the scope of what subsystems should we apply the impact categorizations to. List of what must be included and categorized
- Impact criteria- high level only is the focus. List will help entities come up with list of subsystems that are required to be impact categorized.
- E.g. control and operation function-

- Would it be more beneficial- Should the mapping subgroup requirements fall under these? May not map to the functions.
- Some mapping criteria for every functions? Perhaps but extremely cumbersome and obtuse.
- Invested lots of effort in these functions to center the standards around. If we use these functions to get the subsystems it will move the complexity to Jackie's subgroup.
- This 3rd level of detail looks like BES sub systems. E.g. protection systems down to detail, sounds like a BES subsystem.
- Used these to trigger what we were thinking.
- This has been good work but the SDT is struggling with where are we going with this? What is the vision we are trying to put these pieces together to do?
- Take first one and flow all the way through. See how it might work.
- Keep looking for the integration of the problems/challenges.

2. Day Two Report

- The subgroup has redistributed its members into other subgroups.
- We will continue to try to put more definitions around what was meant by different functions.

Member Comments

- What we have from the subgroup is a list of functions. It would be helpful to have a brief paragraph on each and what is meant for benefit of and guidance to the other subgroups.

B. List of BES Subsystems/BES Cyber systems Subgroup Report and Reflections on Industry Comments, *Jackie Collett*

1. Day One Report

Jackie Collett noted the subgroup had no further meetings since the August Charlotte meeting. She noted that Jim Case and Matt Greek from Operating Committee are now participating on the subgroup.

2. Day Two Report

Jackie Collett presented the Subgroup's report on day two noting that they still need to put time and effort in defining what these BES subsystems are and move into drafting requirements.

Member Comments

- Consider some of these things for simplification on part of this? Requirements based on reliability functions- identify things they are doing that are more important. Maybe on the cyber assets.
- Agree- 2 modes of impact on BES assets and systems. Are we going to continue along both modes of analysis? If not, are we going to utilize impact assessment of both cyber assets and systems? Simplify the two impact analysis.
- BES identification of assets and impact analysis of BES assets.
- Streamline one of those impact analysis. Impact analysis of the cyber system. Will be utilize the output. So they get appropriate direction from the meeting.
- Concern about removing a necessary part of what we are doing.
- Simplify the process. Need to fill in a few more gaps. Look at some of these issues. Don't have all the pieces. This won't be simple. Need to have something that ultimately looks simple.
- Some gaps that need to be filled in. BES subsystem side work. Look at JL's work has done in detail.
- Try to determine where you get any simpler.
- May be an issue that we need to explain how we got to where we are.
- A lot of the complexity in the process is work the SDT has to do. Not necessarily what gets into the standard. Concept paper was similar to this as well. Get requirements on paper that are simple for entities to follow.
- Agree. Identified an ideal vision- down to a "cable driven" methodology. Team still has to go through the exercise. The gaps need to be identified since they will guide the empirical thresholds we need to establish.

Jackie concluded noting they would not say no to volunteers joining them on the work ahead.

C. BES Mapping Subgroup Report and Reflections on Industry Comments, *John Lim*

1. Day One Report

The Subgroup met September 3, 2009 to continue its work in developing the BES Mapping draft markup. The Subgroup was joined by members from the Functions subgroup. John noted two major issues the subgroup is dealing with:

- How do we validate an engineering study? Approval by regional reliability assurer? TFE type process? Need to look at this more. Not a lot of entities currently performing the role of reliability assurer.
- "Misuse"- need to describe this term. What is meant by this? Candidate for NERC Glossary

2.1.6- This addresses how transmission operators or owners classify as high if servicing a generation owner. Currently doesn't have to notify owners of the impact status of their BES systems. This might be an overall point or spread throughout. Thresholds- we can use as long as they are based on some method for the entity. Needs to be the possibility of a challenge of validity through engineering study. Use the numbers with some caveats?

Member comments

- Validation of engineering studies? A number of places reference this. How is this done?
- 3rd party approval is probably not the right approach. Big issue in terms of quality control.
- Can't have "fill in the blank" standards according to FERC. E.g. Regions will develop something everyone in region will have to follow. What we can do, NERC wide standard with different thresholds for different regions or interconnections.
- One of the changes in this version- Eastern and Western and other interconnections might have different thresholds.
- Criteria combines identification of functions and subsystems? Make the process less complex. Would it make sense to do a gap analysis on this criteria? Would reduce complexity.
- Welcome the reduction of complexity. 19 different criteria for this piece alone. How can we compress and simplify? If gap analysis can do this we should explore.
- Concerned that this drafting team puts out hard numbers without engineering analysis behind it. Somehow we need to address this head on.
- These numbers will have to have an engineering basis.

2. Day Two Report

John Lim reported following the Subgroup's meeting on day two. The Subgroup is drafting a set of requirements for High, Medium, Low. There are still questions on how to handle industry studies. In terms of generation sub systems, we are using terms that are not very well defined. E.g. subsystems in generating stations. The terminology we are using must be precise and consistent. We need to get together with Jackie Collett's subgroup. We don't believe there should be an expectation of a 1-to-1 mapping for every function. The rest of the subgroup's work will need to be coordinated with Jackie's subgroup and include input from John Varnell's functions subgroup and from the OC and PCs get something in a better form. Subgroup 1 has participated in past meetings.

D. Cyber Analysis Subgroup Report, and Reflections on Industry Comments, *Phil Huff*

1. Day One Report

Phil Huff delivered the initial report noting his confusion about how the subgroup should go forward. BES impact categorization as the black box is a failed assumption. Our team could reduce some of the complexity in the process. We assumed each function mapped would have an impact categorization so we could combine through a "look-up table."

Member Comments

- External cyber system- address that as a control?
- Target of protection- no requirement just trying to get definition down.

- Our problem is that we are dependent on how the pieces fit together.
- We should focus on impact subsystem.
- Need to determine what we are going to do with the reliability functions.
- Our team's confusion results from the fact that we don't have a clear vision as to how this fits together.

2. Day Two Report

Phil Huff noted that his subgroup would huddle when the SDT breaks. He noted that there may not be as much confusion as we stated yesterday. Impact criteria that are involved in John Lim's one-to-one mapping. Our team needs to develop on the cyber analysis side.

E. Definition and Selection of Controls Subgroup Report and Reflections on Industry Comments, *Keith Stouffer*

1. Day One Report

Keith Stoffer presented the subgroup's report. He noted that during Charlotte meeting the subgroup developed and presented an example based access control. We pulled together into one location the access control referenced in many places. Keith mentioned that the format is new and the subgroup doesn't know if this is acceptable. Need to nail down as soon as possible what is an acceptable format.

Member Comments

- Scott Mix noted an informal discussion with Gerry Adamski at NERC who indicated an openness to doing something to meet requirements. Front of each. Note the categorizations that it applies to.
- Have a table and checkmarks for those that apply.
- Use e.g. re-format.
- Access control- come up with sample sets, won't be meaningful until related to.

2. Day Two Report

The Subgroup will seek to nail the format decision down with NERC. E.g. exemptions. How we deal with conditional requirements? How do we deal with "Requirement"- H/M/L Critical path. What if we run into a brick wall? This is challenging as it is a moving target. Joe Buchiero will send latest work in progress of the Subgroup to all group leaders.

Member Comment

- Select an e.g. that has differences between high, medium and low.

VI. NEXT STEPS AND CLOSING

A. Industry Comments Review and SDT Response

- We will need to take regional differences into account in the standards.
- We haven't yet determined whether there is a null set or just H/M/L. Big issue we need to come to consensus on early.
- Concerns around increasing scope of what we are doing. Have to address this.

Gerry Freese agreed to draft a statement on behalf of the SDT for publication in NERC's newsletter thanking the industry for their input on the concept.

The Chair reviewed with the SDT the schedule for the next couple of meetings reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP 002 which we can refine in November and December. She thanked the members for their hard work together and in the Subgroups and encouraged them to continue working to make headway on each of their charges.

She noted that she would draft up the letter to the Standards Committee Chair based on the SDT's discussion of the TFE and Urgent Action approach at the August meeting.

Members completed an onsite meeting evaluation form *(See, Appendix #3).*

The SDT adjourned at 3:45 p.m. on September 10.

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
14th Meeting Agenda
September 9, 2009, Wednesday - 8 AM to 5 PM PDT
September 10, 2009, Thursday - 8 AM to 5 PM PDT
Western Area Power Administration, Sierra Nevada Regional Office
114 Parkshore Drive
Folsom, California
(916-353-4416)
NOTE: Subgroup Meetings May Not Have Access to Telephones and WebEx

Proposed Meeting Objectives/Outcomes

- Review the CIP 002 Workplan going forward
- Receive updates on TFE, VSL/VRF and related cyber security efforts
- Receive an overview of industry comments on the SDT concept paper
- Receive and discuss reports from CIP 002 Subgroups identifying key issues and coordination points
- Convene CIP 002 Subgroup meetings
- Receive and discuss Subgroup reports on progress made and responses to industry comments
- Agree on Workplan, next steps and assignments

Draft Agenda

Wednesday September 9, 2009

8:00 a.m.	Welcome and Opening Remarks- *Jeri Domingo-Brewer* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review of August 20-21 Charlotte meeting summary and adoption
8:20	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Jeri Domingo Brewer and Bob Jones*
8:30	Review of CIP 002 Workplan and CIP 002 Subgroup Process- *Stu Langton*
8:40	Webinar Report- *Jackie Collett & Phil Huff & Jeri Domingo Brewer*
8:45	Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure – *Jeri Domingo Brewer and Scott Mix*
9:15	Update on VSLs/VRFs- *David Taylor or Scott Mix*
9:20	Update on other related cyber security initiatives- *SDT Members*
9:30	Overview of the Industry Comments on the Concept Paper- *Scott Mix*
10:00	Subgroup Reports to the SDT 1. Reliability Functions Subgroup Report and Reflections on Industry Comments, *John Varnell,* Q & A
10:40	*Break*
10:55	2. List of BES Subsystems/BES Cyber systems Subgroup Report and Reflections on Industry Comments, *Jackie Collett*, Q & A

11:35	3. BES Mapping Subgroup Report and Reflections on Industry Comments, *John Lim* Q & A
12:15	*Lunch*
1:00	4. Cyber Analysis Subgroup Report, and Reflections on Industry Comments, *Joe Doetzl*, Q & A
1:40	5. Definition and Selection of Controls Subgroup Report and Reflections on Industry Comments, *Keith Stouffer*, Q & A
2:20	Coordination Discussions and Plans among Sub Groups
2:45	Subgroup Meetings *(at various locations)*
5:00	*Recess*

Thursday **September 10, 2009**

8:00	Subgroup Meetings
11:00	Welcome and Agenda Review- *Jeri Domingo-Brewer*
11:05	Subgroup Reports – *Plenary Session* 1. Reliability Functions Subgroup Report and Reflection on Industry Comments, Q & A
11:50	2. List of BES Subsystems/BES Cyber Systems Subgroup Report and Reflection on Industry Comments, Q & A
12:35	*Working Lunch*
1:00	3. BES Mapping Subgroup Report and Reflection on Industry Comments, Q & A
1:45	4. Cyber Analysis Subgroup Report and Reflection on Industry Comments, Q & A
2:30	5. Definition and Selection of Controls Subgroup Report, Q & A
3:15	Discussion of and Agreement on Subgroup Coordination Strategies
3:30	Review Work Plan- • Review Next Steps for Subgroups and SDT and the creation of a single CIP 002 text
3:50	Review Proposed 2010 Meeting Schedule
4:00	Review October Kansas City, Missouri Meeting Objectives
4:10	Meeting Evaluation
4:30	*Adjourn*

Appendix # 2 Attendees List
September 9-10, 2009 Folsom, CA

Attending in Person — SDT Members

1. Rob Antonishen	Ontario Power Generation (Friday)
2. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
3. Jim Breton	ERCOT
4. Jackie Collett	Manitoba Hydro
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
7. Sharon Edwards	Duke Energy
8. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
10. Frank Kim	Ontario Hydro
11. Christopher A. Peters	ICF International
12. Scott Rosenberger	Luminant Energy
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15.Keith Stouffer	National Institute of Standards & Technology
1. Roger Lampilla	*NERC*
2. Scott Mix	*NERC*
3. Joe Bucciero	*NERC/Bucciero Assoc.*
4. Robert Jones	*FSU/FCRC Consensus Center (Wed. & Thursday)*
5. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

1. Phillip Huff	Arkansas Electric Coop Corporation
2. Rich Kinas	Orlando Utilities Commission
3. Jonathan Stanford	Bonneville Power Administration
4.William Winters	Arizona Public Service, Inc.

SDT Members Unable to Attend

1. David Norton	Entergy
2. Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, Southwest Power Pool
3. John D. Varnell	Technology Director, Tenaska Power Services Co.

Others Attending in Person

Sam Merrill	CERT/SEI
Michael Toecker	BMcD
Peter Schneider	Subnet Solutions

Others Attending via WebEx and Phone

James Bassett	Lafayette
Matt Greek	
Rob Hardiman	
Doug Johnson	ConEd
Bill Johnson	TDI 9-9
Peter Schneider	
Jeff Gillan	ATC
Sam Merrill	9-10

Appendix # 3 — Meeting Evaluation Feedback Summary

CYBER SECURITY ORDER 706 SDT
SEPTEMBER 9-10, 2009, FOLSOM CA
MEETING EVALUATION FEEDBACK FOR INCLUSION IN FACILITATOR'S REPORT

Members used the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree.

1. Please assess the overall meeting.

7.78 The agenda packet was very useful.
6.83 The Webex document display and the audio were effective
8.50 The quality of the meeting facility was good.
7.40 The objectives for the meeting were stated at the outset.
8.30 Overall, the objectives of the meeting were fully achieved.

Were each of the following meeting objectives fully achieved:
7.90 Review the workplan going forward and assess "Version 2.5" possibilities.
8.10 Receive MRC presentation and Leadership Coordination Meeting summary.
7.13 Receive updates on TFE, VSL/VRF and related cyber security efforts;
8.50 Receive and discuss reports from CIP 002 Subroups identifying key issues and coordination points;
9.00 Convene CIP 002 Subroup meetings;
9.20 Receive and discuss Subroup reports on progress made; and
8.80 Agree on Workplan, next steps and assignments.

2. Please tell us how well you believe the Team engaged in the meeting.
8.70 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
9.20 The Facilitators made sure the concerns of all members were heard.
8.30 The Facilitators helped clarify and summarize issues.
7.63 The Facilitators helped members build consensus.
9.10 The Facilitators made sure the concerns of all participants were heard.
8.10 The Facilitators helped us arrange our time well.

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

8.11 Overall, I am very satisfied with the results of the meeting.
8.13 Overall, the design of the meeting agenda was effective.
8.22 I was very satisfied with the services provided by the Facilitators.
7.89 I am satisfied with the outcome of the meeting.
7.25 I am satisfied with the progress we are making as a Team.
8.75 I know what the next steps following this meeting will be.

8.75 I know who is responsible for the next steps.

See other side

4. Other comments (use other side)

- Small groups good!
- I'd like the sub-teams to do most work offline rather than taking most of our time in sub-team meetings. We need more time together as a group reviewing each other's work and integrating it.
- The inclusion of additional personnel with operating experience was helpful.
- No space on the other side! Until everyone sees responses from the paper we are doing make-work. I believe our over all direction will change when we see the replays. I am a lemming running over the cliff because the facilitators don't know the subject and history. Jerry, Kevin, Jon D, Philip only know normal IT processes.

What did we achieve?

- Make work
- Concrete work on CIP 002

What are our biggest challenges going forward?

- Finishing the amount of work within time parameters.
- Teaching history.
- A coherent/consistent and clear CIP 002.

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

- Sub-team meetings are difficult without projectors.
- Much work is being done in sub-team Silos. This approach created some of the issues with CIP v1. More coordination is required among the various teams to ensure all issues are addressed but NOT addressed by multiple teams.

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

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

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subroups)

should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

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

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

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

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

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

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

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

APPENDIX # 5
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 plenary session to review, refine, and adopt SDT Working Paper
- Adopt SDT response to NERC for Interpretation of CIP-006-1
- Review and adopt proposal for CIP-002 Subgroups and Deliverables
- Convene subgroup organizational meetings to develop work plans
- Adopt 2010 Meeting Schedule

July–August Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting (as needed)

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 Plenary session to review and respond to MRC input on Working Paper/CIP-002 Concepts
- 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 WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

14. September 9–10, 2009 in Folsom, CA

- SDT plenary session to review and respond to any additional industry comments on Working Paper and CIP-002 Concepts
- SDT subgroup drafting meetings- consider industry comments, draft requirements and "proof of concept" control (s).
- SDT plenary session(s) Subgroup reports on requirements
- Review of CIP-002 Standards, Requirements, Measures, and Outline
- Address coordinating issues.
- Establish SDT meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- 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 20–21 — Wednesday–Thursday, Atlanta GA	July 14–15, Wednesday–Thursday
February 18–19 —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