

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

May 13, 2009 | 8 a.m. – 5 p.m. PST

May 14, 2009 | 8 a.m. – 5 p.m. PST

Boulder City, Nevada

**Robert Jones, Hal Beardall and Stuart Langton,
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

**Cyber Security Order 706 Standard Drafting Team
 Draft 10th Meeting Summary,
 May 13-14, 2009
 Boulder City, NV**

| | |
|---|----|
| MEETING SUMMARY CONTENTS | |
| Cover | 1 |
| Contents | 2 |
| EXECUTIVE SUMMARY | 3 |
| I. INTRODUCTIONS, AGENDA REVIEW AND REVIEW OF SDT WORK PLAN | 7 |
| II. UPDATE ON MRC PRESENTATION | 7 |
| III. TECHNICAL FEASIBILITY EXCEPTION UPDATE AND SDT DISCUSSION | 8 |
| IV. VSL AND VSR SDT UPDATE | 10 |
| V. UPDATE ON KEY MESSAGES TASK GROUP | 10 |
| VI. SDT 706 PHASE II/VERSION 3 DEVELOPMENT PROCESS - THE WORKING PAPER | 10 |
| A. Overview of Phase II Work plan | 10 |
| B. Working Paper Presentation and Review | 12 |
| C. SDT Phase Working Paper Development - Day Two | 19 |
| D. SDT Phase Working Paper Development Process Going Forward | 24 |
| VII. NEXT STEPS | 26 |
| A. 2009 Work plan Approach | 26 |
| B. Work plan Schedule | 26 |
| C. White Paper Development | 26 |
| D. Process and Meeting Evaluation | 26 |
| Appendix 1: Meeting Agenda | 27 |
| Appendix 2: Meeting Attendees List | 29 |
| Appendix 3: Meeting Evaluation Summary | 31 |
| Appendix 4: NERC Antitrust Guidelines | 33 |
| Appendix 5: SDT Work plan Schedule | 35 |
| Appendix 6: Working Paper: Categorizing Cyber Assets: An Approach Based on BES Reliability Functions | 38 |
| Appendix 7: SDT Process Survey Executive Summary and Recommendations | 39 |

**Cyber Security Order 706 Standard Drafting Team
Draft Eighth Meeting Summary,
May 13-14, 2009
Boulder City, NV**

EXECUTIVE SUMMARY

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 for each day. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the Team and participants the proposed meeting agenda.

Mr. Bucciero reviewed with the Team the need to comply with NERC's Antitrust Guidelines including avoiding behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion. The Team reviewed and unanimously adopted on the SDT 706 April 14-16, 2009 meeting summary with editorial corrections suggested by the Vice Chair. The Chair and Vice Chair welcomed Jim Breton as a newly appointed member of the SDT representing ISO perspectives. The Chair then congratulated the SDT members on the overwhelming industry approval of the Phase I package of changes to the CIP 002-009 (April 17-27 Recirculation Results: Quorum: 94.37 percent Approval: 88.32 percent). Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule Phase 2.

The Chair noted that she was unable to present to the MRC but Jim Breton noted he was present and that the SDT materials were well received by the MRC.

Scott Mix provided an update briefing to the SDT noting that the posting period closed for the TFE had closed with 52 organizations providing comments over 450 pages. He said that NERC staff is now analyzing the comments. All comments have been posted on NERC web site. Mr. Mix noted there were concerns over the 60-day automatic approval and issues concerning where a TFE can be applied. Members reviewed the history of the TFE process and the SDT's role in their development and clarified the procedural and substantive implications of the TFEs for the CIP 002-009 standards development.

David Taylor, NERC, provided an update on the VSL/VSRs. Since the last meeting they were posted out for industry comment. The comment period is now closed and the 93 pages of comment from 10 entities are being reviewed by the SAR drafting team at their meeting on May 14, 2009.

Version 1 and 2 VSLs must be filed by July 1.

Gerry Freese presented an update from the “Key Messages” discussion at the April SDT meeting in Charlotte. He noted there was perhaps less emphasis than last time given the flood a media attention in April. Members discussed the fact that there were several bills that had been filed in both the Senate and House that focus on different aspects of cyber security policy including the Senators Snow and Rockefeller bill that focuses on Education - R&D, a Senators Bingaman, Lieberman and Thompson bill and a bill Markey is working on in the House.

Michael Assante noted that NERC had been focused on developing key points for Rick Sergel’s (President, NERC) testimony in the past weeks. He suggested that there was still value in having good communications and engaging with congressional staff on pending legislation. Gerry agreed to share his draft with the sub team and bring it back on the second day for considerations regarding next steps. On Day Two he agreed to work with the Key Messages Team in refining this and developing a strategy going forward.

Stu Langton reviewed with the SDT the milestones in Phase 1 and Phase 2 of the SDT. The facilitators made a suggestion to consider calling this a “working paper” as the term “white paper” suggested a less dynamic, more static state. The working paper provided a basis for developing the consensus points that were tested and refined in April at the Charlotte meeting.

The Vice Chair proposed the SDT’s consideration of a different timeline for CIP 002. The current proposal seeks industry comment on CIP 002 by the end of the year but then develops CIP 003-009 before going out for ballot. Instead consider taking CIP 002 for ballot when ready. In terms of the implementation plan, limit it to those assets considered high and continue to apply the existing CIP 003-009 until they are redrafted. This approach gets improved asset protection out faster. Wouldn’t cause anyone to lose under existing standards. The SDT members discussed this option and left it open for further consideration.

The SDT discussed when it would be timely to consider whether to maintain the current CIP structure 002-009 or consider streamlining and addressing overlaps and duplication and possibly creating one set of standards.

The facilitators summarized the discussion of possible directions and next steps. First there appeared to be SDT support for getting out the new CIP 002 as early as possible for comment, refinements, and on to ballot. As the SDT develops CIP 002 with measures and requirements, it will need to address how it wants to develop the structure for the present CIP 003-009. The suggestion was made to review all of these issues at the next meeting and to talk about our schedule and strategy.

The Chair thanked John Lim, Phil Huff and their drafting team for working hard since the Charlotte SDT meeting and expressed on behalf of the SDT her gratitude for their leadership and good effort. John Lim, Phil Huff, Jackie Collett and Bill Winters jointly presented the next draft of the Phase 2 Working Paper. They noted the expanded team met twice by phone-WebEx following the Charlotte meeting. They noted they cleaned up the introduction and sought to expand some sections based on the SDT discussion in April. They underscored the fact that there remain significant gaps in the documents, in particular: the critical assets categorization

methodology; and the criteria for categorization of the cyber assets. They have tried to define a couple of additional terms. Overall, the team is not very close to finalizing the document. The members discussed the fact that the evolving document has been made accessible to industry and that it is already being broadly discussed. The SDT needs to be prepared to address inquiries as it continues to refine this document.

The SDT reviewed, discussed and offered suggestions for each section of the working paper including sections addressing: Introduction; the Terms and Definitions; BES Reliability Functions; Identification of BES Subsystems; Categorization of BES Subsystems; Third Party Oversight; Identification of Essential Cyber Systems; Categorization of Cyber Systems; Cyber System Interconnections; Final Categorization of Cyber System Based on Overall Impact on the BES; Risk Based Approach to Security Control Selection; and Effect of Cyber Systems Categorization on Requirements

On Day two the facilitators reviewed the following SDT areas of possible agreement with the Working Paper approach and concepts from the Day One SDT discussion:

- Recognize different audiences: develop Executive Overview (e.g., will have to protect more assets than before; will require identification of more BES assets than did before; will require different levels of protection) that clarifies the intent at a high level regarding methodology;
- Address structured and unstructured threats;
- Develop graphic and tabular depictions of key concepts in white paper;
- Terms and definitions- take a step back and address in content sections;
- Address connectivity as an important concept;
- Seek outside assistance from operating and planning committees for identifying and categorizing BES sub systems and reliability function; and
- Categorize the cyber systems.

The facilitators suggested that the following were outstanding Working Paper issues from the Day One discussion, some of which could be taken up in small group discussions. The SDT reviewed the 3rd Party Review section and ultimately agreed to clarify how much ability each entity has to categorize BES subsystems and what kinds of overview is intended.

The SDT worked in small groups to further explore and refine the issues and options surrounding:

- Identification of Essential Cyber Systems
- Risk Based Approach to Security Control Selection; and
- A third small group participated in a phone conference with FERC staff regarding an issue that was discussed under the Technical Feasibility Exception.

In general, going forward the SDT agreed that the Working Paper focus should be on the overall approach to the CIP-002 issues. The drafting team agreed to continue working on refining the working paper including taking a more conceptual approach while holding the details for

consideration as the SDT begins development of the new CIP 002. Categorization of the BES assets still needs refinement and help from outside experts. Scott Mix and Joe Bucciero will take the lead to see if additional expertise can be provided to the sub team.

Bob Jones, SDT facilitator, noted the proposal to proceed with CIP 002's development in the remaining half of 2009 and refine it after a sequence of comments from the industry before going to the ballot. The Chair reminded people to register for the Portland Bonneville Power meeting and that the July meeting would take place in Vancouver, B.C., Canada.

Hal Beardall reviewed with the SDT the results of the process survey undertaken in March and April. Following the review, Stu Langton led an onsite meeting evaluation discussion and members completed written evaluation forms.

The SDT adjourned at 3:45 p.m. on May 14.



The SDT Order 706 turns a corner in Boulder City

**Cyber Security Order 706 Standard Drafting Team
DRAFT TENTH MEETING SUMMARY,
MAY 13-14, 2009
BOULDER CITY, NEVADA**

I. INTRODUCTIONS, AGENDA REVIEW AND REVIEW OF SDT WORKPLAN

The Chair, Jeri Domingo-Brewer, welcomed the members at 8:30 a.m. having been delayed by technical problems with the WebEx and phone. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day (See appendix #2). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the Team and participants the proposed meeting agenda (See appendix #1).

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

The Team reviewed and unanimously adopted on the SDT 706 April 14-16, 2009 meeting summary with editorial corrections suggested by the Vice Chair. The Chair and Vice Chair then welcomed Jim Brenton as a newly appointed member of the SDT representing ISO perspectives.

The Chair congratulated the SDT members on the overwhelming industry approval of the Phase I package of changes to the CIP 002-009 (April 17-27 Recirculation Results: Quorum: 94.37 percent Approval: 88.32 percent). Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for Phase 2. (See Appendix #4) The Chair noted that the location for the SDT July meeting would be in Vancouver, Canada.

II. UPDATE ON NERC MEMBER REPRESENTATIVE COMMITTEE MAY 5, 2009 PRESENTATION

The Chair noted that she was prepared but unable to present as she was ill. Jim Brenton noted he was present and that the SDT materials were well received by the MRC. At this juncture the MRC did not have feedback for the SDT. SDT Members requested that the written presentation materials including a power point be circulated to them and the Chair agreed to do so.

III. UPDATE ON TECHNICAL FEASIBILITY EXCEPTION (TFE) NERC RULES OF PROCEDURE POSTING

Scott Mix provided an update briefing to the SDT noting that the posting period closed for the TFE had closed with 52 organizations providing comments over 450 pages. He said that NERC staff is now analyzing the comments. All comments have been posted on NERC web site. Mr. Mix agreed to send a link to the members. Some of the common themes in the comments included:

- Concerns over the 60-day automatic approval which no one appeared to like.
- Issues around the requirements where a TFE can be applied.

NERC staff is now reviewing and considering modifications and will try to get this done as quickly as possible. Mike Assante, the NERC CSO is the Corporate Officer in charge of content. Dave Cook, NERC General Counsel is in charge of procedure. Mr. Mix noted that the Edison Electric Institute had submitted both a redline version change to the appendix. The SAR hasn't been submitted as of yet to the standards committee.

Member Discussion Comments on TFE Update

- Version 1 of standards compliance July 1. Version 2 effective date kicks in after FERC approves the standards.
- Canadian entities without regulation (e.g. Manitoba) January 1, 2010 is the effective date for the Version 2 CIP Standards.
- Is there a compliance gap? It is a self report, as before.
- "Version 1 of CIP standards- auditably compliant by July 1, 2009.
- "Reasonable business judgment"- what does it provide entities now?
- Roger Lampila, NERC Compliance, indicated that by taking away reasonable business judgment the auditor will determine if you used reasonable business judgment. Always has the appeal.
- Version 1- "what's the shell game"? TFE draft- could apply to other reliability standards not just CIP? Yet it seems to be all about CIP. Industry will want to see this in the CIP standard.
- If it is in the standard, there needs to be a requirement around a TFE process that compliance could hold you to.
- The TFE has not been approved yet by the NERC BOT nor filed with FERC. This is to get NERC/industry started in the rules of procedure. What do you do now? Self report, the same as before.
- Why are we amending the blanket rules of procedure with language specific to CIP? Why not write this more generically?
- Mike Assante noted that NERC will be responding to the comments.
- No other standard has the triggering language. Don't want a blanket exception in CIP or at large. That is what NERC is trying to prevent. E.g. TFE tree trimming, etc.
- TFE makes more formally recognized process within mitigation plan. Changing the cover page. From a regional entity perspective, today NERC receives, evaluates approves/rejects TFE.

- What should the role be for the regional entity?
- Given TFE says can't ask for TFE unless standard says you can. Do we have to do through a separate SAR or can the group do this under our charter. Limited focus, placement of TFE in the standard?
- SAR should allow the SDT to address TFE where appropriate. David Taylor indicated that he would recommend to the Standards Committee that the SDT have ability to do so in the current SAR. It would take a lot of discussion to determine which requirements this should apply to.
- If the group wanted to do it would be an appropriate thing. Possible consider doing this in a SDT subcommittee - could do this. This will not be a trivial or easy task for the SDT. If it is the right thing to do we should do it even if it will take time to complete.
- Industry is between rock and hard place - if need for TFE and standard doesn't permit.
- TFE has to be approved and in place. Could be part of the SDT's Phase II, (i.e. Version 3) of standards.
- The SDT should come back to this and do some preparation and thinking regarding how to frame and how to organize to get the work done.
- NERC and RE role in evaluation? There are industry comments on that and NERC staff will be responding.
- Mike Assante noted that there has been discussion in the industry on whether there will be modifications where RE's could play a different or bigger role and its budget implications.
- There are some practical issues with the FERC order and the TFE: e.g. the 24 hr removal of access after termination for cause. Proceeded on assumption - remove access. Isn't a TFE designed to take care of this? Puts in non-compliance. 706 said 24 hours was too long. Can't be done practically. Could have addressed some of these issues in version 2 and will need to address this in Version 3. Is there a way we can address, "All assets"?
- Version 1 issue - TFE, document through self report.
- E.g. password - exception against own compliance policy and a TFE against standard. "Where technically feasible" - No process to file at TFE. Have to do self-reported compliance.
- Where requirement allows TFE exception - do I have to file a compliance exception separately. In 007 or e.g. 005 R3.2. Doesn't specify exception. This one tells you what to do in the requirement. Others don't.
- What you have written into a policy.
- You can see the level of TFE contention in the SDT and this is also happening in the industry. Lots of questions around this "can of worms."
- TFE concerns - version 1 and 2 going forward. Time takes to respond when standards have specificity. We could go through with blanket statement - take TFE where applicable. Changes in technology. With reasonable business judgment stripped away. Limit TFEs to a limited number of standards with changing technology will be a losing proposition. Should approach more generally. Shouldn't specify only certain places.
- If you take away physical and network access, you have removed access and fix other policies.

- Compliance auditors only audit to standards and not to policies.
- Version 2 - BOT approved in May, 09. Canadians need to file with regulatory authorities. Effective date - 1st day of 3rd quarter. (i.e. Jan. 1, 2010).
- Communication to industry - let everyone know when things become effective. There is confusion. For any new standards what is the effective date. NERC needs to get info out on TFE's.
- Can't take a TFE until then. Self report of non-compliance with a mitigation plan. E.g. Passwords - 6 characters. CIP 007 R5.3 "as technically feasible". If device supports only 4 characters. Required by standards to do anything? What was the intent? 4 position password. Would have to demonstrate why only using 4- produce industry.
- In the meantime perhaps the SDT can put together an explicit document - here is what you need to do. Focus on what does the industry need to do today. This is what enforceable at what dates.
- Industry and auditors don't know how to handle these.

IV. UPDATE ON VSLs/VSRs -

David Taylor, NERC, provided an update on the VSL/VSRs. Since the last meeting they were posted out for industry comment. The comment period is now closed and the 93 pages of comment from 10 entities are being reviewed by the SAR drafting team at their meeting on May 14, 2009.

Version 1 & 2 VSLs must be filed by July 1. Didn't receive a lot of comments on Version 2. Asked questions about changes in VRS. Didn't receive comments. These will soon get out for ballot/recirculation.

V. UPDATE ON THE "KEY MESSAGES" TASK GROUP

Gerry Freese presented an update from the "Key Messages" discussion at the April SDT meeting in Charlotte. He noted there was perhaps less emphasis than last time given the flood of media attention in April. Members discussed the fact that there were several bills that had been filed in both the Senate and House that focus on different aspects of cyber security policy including the Senators Snow and Rockefeller bill that focuses on Education/R&D, a Senators Bingaman, Lieberman and Thompson bill and a bill Markey is working on in the House. All want cyber security but the question is how to fund this. Concern about the industry being log-rolled with a poorly designed solution. Need to identify who is the driving force and find that out and seek out their staff for the key messages.

Mr. Freese noted that he went on vacation immediately following the Charlotte meeting. He has since put together presentation which he suggested showing to those who agreed to work with him on the "team" which included John Stanford, Jerry Domingo Brewer, Jay Cribb, Dave Norton, Phil Huff, Rich Kinas and Jim Brenton. He asked the Team and Michael Assante if this was still worthwhile going forward with. Michael Assante noted NERC had been focused on key points for Rick Sergel's (President, NERC) testimony in the past weeks. He suggested that there was still value in having good communications and engaging with congressional staff on pending

legislation. Gerry agreed to share his draft with the sub team and bring it back on the second day for considerations regarding next steps. On Day Two Gerry noted he had inadvertently sent the draft out to the SDT plus list. He agreed to work with the Key Messages Team in refining this and developing a strategy going forward.

VI. SDT PHASE II/VERSION 3 DEVELOPMENT PROCESS- THE “WORKING PAPER”

A. Overview of Phase II/Version 3 Work Plan

Stu Langton reviewed with the SDT the milestones in Phase 1 and Phase 2 of the SDT work including the work in Little Rock to begin to frame the challenges, the development of “white papers” following the Washington D.C. meeting in December and further review and refinement of those and other papers and the convergence on an single consensus approach in Orlando that was refined further in Charlotte with John Lim and Phil Huff leading a team to continue to refine the white paper. The facilitators made a suggestion to consider calling this a “working paper” as the term “white paper” suggested a less dynamic, more static state. The paper provided a basis for developing the consensus points that were tested and refined in April and offered to the industry Members Representative Committee.

Member Discussion of Progress To Date

Overall

- Congress - wants to see standards that protect all the control networks.
- What congress will do or not do shouldn't drive the SDT process, rather the SDT should seek to do the “right thing.”
- Productivity in working together as a group - confidence in producing a lot and working at a good pace.
- At the end of the day NERC - industry should be in control of the shaping of the CIP standards.

CIP 002 Workplan - Go to Comment and Ballot First with a Complete CIP 002.

- The Vice Chair proposed the SDT's consideration of a different timeline for CIP 002. The current proposal seeks industry comment on 002 by the end of the year but then develops 003-009 before going out for ballot. Instead consider taking CIP 002 for ballot when ready. In terms of the implementation plan, limit it to those assets considered high and continue to apply the existing 3-9 apply until we get they get redone. This gets improved asset protection out faster. Wouldn't cause anyone to lose under existing standards.
- The idea of completing CIP 002 makes sense. Nobody can tell us what CIP 002 should be. Congress could say “secure all.” Nobody can do this for us. In following the Smart Grid Task Group - there are many consultants but few industry representatives there.
- CIP 002 is the big ticket item for the industry. The SDT effort to tackle CIP 002 can provide leadership guidance to Smart Grid group. May need to jump in on that? \$4.3 billion is

devoted to supporting its development. By getting the scope and methodology in CIP 002 earlier we will help provide leadership for other efforts including NASBEE.

- CIP 002 - angst with Version 1 and 2. Doubts regarding industry's willingness to adopt without 003-009. May need to know about controls and effect on controls.
- CIP 002 - critical asset identification is a challenge but the SDT should make this happen quickly and deliver.
- Got to get past the industry push back. We should be doing the right thing. Won't be an easy process.
- Scott Mix suggested that procedurally it would not be a big issue in going to ballot on CIP 002 first. Would need to make clear on the impacts with other standards. Assuming the first draft is out for comment in December, will probably take multiple times back and forth responding to industry comments before going to the ballot with CIP 002. In the meantime during 2010 the SDT could be working in parallel making headway on CIP 003-009.

Structure of CIP 002-009

- Are we stuck with 002-009 Standards structure? Can we think about 1 set of standards? There are problems with the structure of current standards? Give consideration to putting into one set?
- All NERC standards have a family and sequence number.
- Structure of CIP 002-009. This works together- structure is there is you read the whole thing.
- Renumbering the standards - straighten out. List existing, list by categories. Cross-referencing makes interpretation difficult. Industry willing to spend \$ just needs to know what to spend it on.
- There may be more understanding - on structure than is suggested by the discussion. Careful not to throw out the baby with the bathwater.
- Jon Southern noted he was not suggesting that. There are some overlapping and duplicative aspects to the current structure, e.g. audit logging in several sections. 005 and 006 are circular. NIST doesn't have this issue. The movement is to view cyber security assets more holistically as correlating systems.

The facilitators summarized the discussion of two possible directions and next steps. First there appeared to be SDT support for getting out the CIP 002 as early as possible for comment, refinements and on to ballot. As the SDT develops CIP 002 with measures and requirements, it will need to address how it wants to develop the structure for the present CIP 003-009. The suggestion was made to review all of these issues at the next meeting and to talk about our schedule and strategy.

B. Phase II Working Paper Presentation and Discussions

The Chair thanked John Lim, Phil and their team for working productively since the Charlotte SDT meeting and expressed on behalf of the SDT her gratitude for their leadership and good effort. John Lim, Phil Huff, Jackie Collett and Bill Winters jointly presented the next draft of the Phase II Working Paper (See Appendix #6) They noted the expanded team met twice by phone-WebEx following the Charlotte meeting. They pointed out that they cleaned up the introduction

and sought to expand some sections based on the SDT discussion in April. They underscored the fact that there remain significant gaps in the documents, in particular, the critical assets categorization methodology and the criteria for categorization of the cyber assets. They have tried to define a couple of additional terms. Overall, they suggested the drafting team was not close to finalizing the document yet and that there were a number of issues the SDT needed to address and resolve. The members discussed the fact that the evolving document is accessible to industry and that it is already being discussed. The SDT needs to be prepared to address inquiries as it continues to refine this document and minimize any confusion that making the evolving draft available might cause.

1. Overall SDT Comments on Working Paper

The Team engaged in an initial discussion of the working paper. A summary of their comments are noted below:

- Industry is interested in what we are doing. Asset identification. Compress the timeline. Sooner the better.
- Consciously stayed away from reviewing the paper until this draft. Through 1st half. Struck by definitions and some more later. Could we create a taxonomy of the terms? E.g. a BES system can be used in different ways. Diagram showing the logical relationship of high order concepts,
- Members should consider this a very early draft that still includes some contradictory statements and inconsistency on terms.
- Scott Mix reported on his discussions with Operating Committee members to help the SDT with the engineering side of the analysis. Big topic last week. Lack of inability to participate in the standards process. Will be well received by the Committee members and hope we will get some who can participate. Won't get names from the Committee until mid June which will be just before Portland. If goal is to have a draft good enough for industry comment. Hold off a month to get the benefit of the Committee members input.

2. Introduction- Section

- The Team cleaned up and accepted changes suggested from the April meeting. Not much new work in the Introduction.

Member Comments and Suggestions

- Reference to the 6 characteristics? Adequacy is the last of the 6? Is that separate and distinct? Problem with implications see it in the table later.
- Reaction of 6 points of the NERC ALR - "reasonably expected" Protect to the normal, vs. protecting for the for unexpected and unplanned in cyber. The focus. Understand focus on ALR - send the wrong message to industry. Emphasize from cyber security.
- Mike Assante noted the same concern - we should think about multiple loss of assets in an abnormal instance.

- Mike Assante's letter of April 6 noted the industry will have to address structured and unstructured threats. The standards will have to be tailored to deal with unstructured. That is how the cyber side works.
- ALR is the granite cornerstone to grow our efforts? If 6 "2. "Credible contingencies". Leave these as they are? If we play with them everywhere.
- "Everything is credible after it happens" pp 12 5 functions - focus on that - forget about other?
- References to previous presentations to SDT - not helpful in current form, because they need to be understood by the reader who hasn't heard those presentations. Consider our audience.
- Illustration diagram-graphically captures the relationship between the 3.

3. Terms and Definitions Section

John Lim and Phil Huff indicated that the drafting Team was trying to ideally define cyber system vs. asset. Realizing the audience, it will be important to delineate an "essential" cyber system from a cyber system. The Drafting Team decided to look at the essential cyber system first to delineate the target of protection and the essential cyber system and determine what is our target of protection when later developing controls.

Member comments

- Define systems (cyber). What is a BES subsystem? Thought about this in pieces - systems vs. assets on both the power system and cyber side.
- Discussion of cyber systems - pp 8- aggregation and segregation. Embellish all applicable cyber assets that need to be slotted into those systems in a logical and manageable way. Point not well made yet in this paper.
- The drafting team grappled with how much do we want to go into that in the terms and definitions section vs. later in substantive sections. May have gone too far in the terms and definition section in this draft. Address this in a content section.
- We may have gotten too detailed, in trying to get the content down first and then think about whether rearranging. Entity allowed to cherry pick?
- Segregation will take you to controls. We were trying to hit a higher level in first run.
- May have to move some of this further into the paper and consider the effects on requirements.
- Perhaps the new terms and concepts can be defined in this section. There is typically some confusion in a technical paper. Maybe in the introductory section address the high level view-framework of what we are trying to say here. Concept of cyber system introduced, drill down later.
- How does the identification work, when will it become clearer? Is the goal of the paper to let industry know what they need to protect?
- No. This is a rough conceptual draft. This section has continued to get less clear with the introduction of new concepts. There is a need for a new taxonomy. Is there any input on whether we have presented a clear enough concept to get reactions? Tripping over things. How far off base are we with the intent?

- This paper's intent is to give an idea of the methodology we are considering. It will say this at a high level. The takeaway for industry is: 1) You will have to protect more assets than before. 2) You will have to identify more BES assets than did before. 3) There will be different levels of protection but you won't get a list yet as this is not a standard but a concept.
- Overview of the approach is needed - executive summary. Introduction doesn't do it yet. It should include Jackie's points. Jackie agreed to write it up.
- Who is the audience we are addressing in the working paper? Technical people? Higher level Execs? Focused intent of what this is about. Jackie's points are perfect for that audience.
- Tried to focus on full gamut of audiences from executive viewpoints and the technical viewpoints. Should we consider breaking this up into 2 papers one for technical folks, one for executive management?
- Take the highest level approach for discussion of the concept which can set the context for details that follow.
- The diagram shows the departure from critical asset. Cyber isn't limited by electronic security perimeter. Proper network segmentation.
- Protection requirement applies to assets not directly part of the BES. Because of "interconnectedness" and FERC's direction, this may end up in assessment and controls. There may be a minimum set of controls to other systems because of the interconnectedness of cyber systems that are used to control them.
- If generation unit, has no impact on BES is it off the table? It would be brought in if you establish its interconnectedness and vulnerability and implementation of minimum set of controls to mitigate.
- Can be separate electronic security parameters. Maybe we can try to get at that with an additional diagram.
- End point security model is another alternative to the perimeter model. That is where CIP 007 comes in?
- RFI team and WEC - integrated firewalls and routers etc. Some discovery in that discussion?

4. BES Reliability Functions

The Drafting Team shared that the intent was to capture work and discussion on critical asset identification of risk assessment working group translation. They hope to get some help from the operating and planning committees and this is a work in progress not intended as final. They are looking for suggestions.

Member Comments

- Criteria in table - criticality and impact factors concern of their appearance here. Credit to Sam Merrill. He is working on a paper of a services approach to critical infrastructure protection.
- With terminology change - might work. (diagram) Is this what we are trying to get at? Consider this? Phil believes this aligns nicely. Overload the term "systems" It should be clear that BES - cyber can be a sub-system of BES. There is no diagram yet to show it can be both.

- Parallel categorization effort presents a concern: BES on one side, cyber on the other and merge later? BES should feed into cyber categorization. May be problematic to do this independently.
- Drafting Team had the same concerns with cyber impact assessment - on the function not on the BES sub system. You don't know to what degree it has an impact on BES. You need to know to what degree high-medium-low affect the BES.
- Come up with some e.g. a protective relay is a cyber system. Whether it's on a 500 kv line, or 115 kv line in middle of nowhere. Same equipment but the impact on BES is different. Put minimum security on 115 kv.
- I like both the diagram and table. Need to present in different ways for different audiences.
- Two concerns: generation too all encompassing. Avoid "other" catch alls in these standards.
- Contingency reserve = single unit bigger than reserve - not all units together? "Biggest unit"? Combined units.
- Drafting Team's intent to signal that lots of generation not included in current assets. It will be more than your black start units but less than everything. We will need help from the Operating and Planning committees. That is hard work ahead.
- Words - use the same label on both tracks. Use other words (assembly, components, etc.)? NERC glossary is a concern. Some of terms we like to use, such as element, doesn't work.
- Relays as cyber systems and be consistent: is connectivity-risk is missing from the document? Don't see it explicitly here. Vulnerability isn't discussed, but impact is. Look at the section: Risk Based Approach to Security Control Selection)
- We are talking about assets and we don't have enough generation on list? That is not the right question. If there is connectivity then maybe all are there. Don't like the approach - if it doesn't provide security - won't be doing the job.
- The paper is trying to relate assets to functions (services approach) which weren't done before.
- We have fuzzy boundaries, generation, transmission, distribution. Turf state and federal. Cyber security view - if you can get into and move up line on a common controls network this is a problem. Smart grid lumped together Transmission and Distribution.
- Capture even with distribution level system that "connect" to transmission and impact reliability of BES.
- The SDT needs to get more involved with the smart grid security task group.

5. Identification of BES Subsystems

The Working Paper characterizes cyber system as a BES asset.

Member Comments

- Is the diagram in original paper clearer? See the outline of the white circle.
- Labels systems - suggestion to make clearer that h/m/l in each transmission, generation

6. Categorization of BES Subsystems

The Working Paper makes no changes in this section since April. The drafting team will get this fleshed out when help comes for the identification BES assets from the Operations and Planning committees.

7. Third Party Oversight

While there were no major changes but a rewrite of the format with some help from Sam Merrill and a clarification of the process for disputes and appeals.

Member Comments

- Focuses approval - oversight on BES engineering side not the cyber side. No oversight provisions on the cyber side.
- What about the Reliability Coordinator role?
- Does this relate to oversight of entities to make up their own rules? Better approach -- the development of regional interconnect wide categorization criteria for BES subsystems. Simplify the process. Map your assets to regional criteria and functions. The categorization is a mapping exercise vs. an oversight exercise.
- Can the paper explore this as an option? Put both options on table making the case for each? Or present to SDT for decision. Does this section currently assume entities will make up own rules?
- Why not be told what the assets are vs. providing the criteria?
- Industry has been involved with this e.g. 100kv. If you go to region to make decision, the entities will be making the criteria. Might be looser criteria if done at the regional level.
- Looking for uniformity around this asset categorization. E.g. Reliance on redundancy, etc.
- Regional criteria for bulk power hasn't worked in other instances.
- This is an idea worth exploring. Weakness in federal model lack of uniformity across federal agencies. This could help industry address CIP 002 process and send a message to congress that the industry is looking at holistic solutions.
- Whoever has responsibility - they should pay the fine if this is not done right. Need to think this through. Don't want to touch this with a 10 ft pool. Policy is no thank you. We determine our critical assets. Lean much towards compliance.
- Categorization is dynamic process. Add and retiring transmission. Continual nightmare keeping a list up-to-date and current.
- Move towards criteria by which multiple entities come to the same conclusion. Three entities with the same equipment should come up with the same solution.
- Why not have the SDT come up with criteria?
- Problem with creating a fill in the blank standard. Dead end. Can we require each region to come up with own independent standard? Have to be able to justify. What would it be?
- Single NERC standard with West, East, ERCOT, nailed at an interconnection level. E.g. criticality of a control center would be same across the three.
- Challenge is you can't audit "reasonability"-- this would bring the entities to the same place. The pass through of the region is to check if something was missed.

- Can we define a criteria that sets minimum expectations. If there are regional differences, there can be a process that will define and justify any differences. Gets away from “reasonableness”, but allows for differences between the regions and their infrastructure to be taken into account.
- A regionally specific standard - can be more stringent than a continent wide standard.
- SDT should come up with a base set of minimum criteria.
- Why have a different set of rules for a region to identify BES subsystems?
- We are trying to run through two sets of filters - will we get the same answer? Focus on categorizing cyber assets side first BES. See if we can categorize those. We have similar e.g. control centers, etc.

8. Identification of Essential Cyber Systems

The Drafting Team noted that the change in the introduction of BES subsystems is consistent with the new definitions. This is the introduction of essential cyber systems.

Member Comments

- Focus is BES and generation - on back end, are the other systems managing those part of this? Coal, gas etc.?
- Fuel inventory managing piles, timelines no. Control over pulverizer-conveyor belt. Possibly?
Does this capture those things?
- Go back to 215 a (1) - doesn't include distribution facilities.
- Essential at this point. Doesn't preclude other systems coming in within the scope of protection.
- “Critical systems”- systems at the control center level are complex. ISO's challenge-zonal vs. nodal markets, market system may be essential to reliability. We have found in working with operations staff that key functions are not always obvious.
- Need to look at this section more closely for its implications.
- Is the market system itself a critical asset? May depend and vary. How you schedule a function may be in or out. Moving towards more integrated systems and this will present a challenge.
- Should we have a list that limits what systems?
- Identifying different levels of protection required. Are we focused too much on BES assets.
- Mindful of as developing the standards, if it is in the standards and there is not fuzziness, then everything is included. Other systems that impact reliability?

9. Categorization of Cyber Systems

The Drafting Team noted that this section was clarified, not substantively added to.

Member Comments

- BES functionality concern - problem regarding lack of clarity is a critical assets. Does it require a wholesale move away?
- With CIP 002 we have learned that one size doesn't fit all. The challenge is in applying good security practices to interrelated assets. This is the cyber security realm.
- The concept proposes a melding of two approaches to meet the security outcomes sought.
- The concept is looking to understand the impacts to the BES functions. Not tying it to BES reliability. That is done however, implicitly, through the matrix.
- Still perform both assessments. BES subsystem assessment feed into.

10. Cyber System Interconnections

Member Comments

- Requirement of standard should be that two parties negotiate an agreement to protect the security device.
- This is in part addressed by the oversight section.
- If utility A has interconnection, then they will address in a service agreement with Utility B.

11. Final Categorization of Cyber System Based on Overall Impact on the BES

Member Comments

- Merging of the categorizations of BES and Cyber to be used for applying of controls appropriate to the level
- Review and clarify the Table- low = no impact and none = consistency. Are low to none the same?
- Start/End.
- BES assets would replace BES sub systems.

12. Risk Based Approach to Security Control Selection

The drafting team asked if they have adequately addressed risk after categorization?

Member Comments

- Provide a framework (similar to NIST) to use to provide your security controls.
- Address what doing with controls - commensurate with the cyber system they will be protecting.
- Overall objective mitigating the risk- high impact system- take what you are trying to protect and reduce the risk commensurate to its impact on the BES.
- Addresses the earlier comment about connectivity.
- Concept of controls - incorporate risk assessment into that construct. Not assuming everyone does their own risk assessment. Perhaps not as extensive as NIST.

- A device that doesn't have impacts but could have. As you change the connectivity. Pick a different control now that you have modified the environment.
- This adds another layer of complications in implementation (3 impact ratings; 5 more)
- 1 size fits all doesn't work. Flexibility should make sense from several perspectives.
- Cyber - less important. Applicable to all BES systems?
- Intent is to significantly address cyber issue.
- Physical security - applicability broad enough to reach beyond cyber. Cyber is a part.
- 1st half of 002 is not a cyber - BES impact method will be
- Security issues - overlaps - categorization exercise sets up for CIP 10 -18 family, physical protection of equipment. Electro mechanical vs. digital.
- Upgrading equipment - don't have to go through the process.
- Unclear section of white paper. Trying to address risk in the writing of the controls addressing different operating environments. Addressing risk in the entity level - applying a vulnerability analysis.
- If we don't know how we are going to do this.
- Trying to write a requirement for this will be very hard.
- Remember Mike Assante's advice to the Team in December: look at what you want to accomplish and then think out of the box on how to get there.
- Focusing on what is our method of identify protections. After feedback, we will move forward flushing out another white paper focusing on the controls and protection.
- Concerned about expectations regarding risk assessments and small entities

13. Effect of Cyber Systems Categorization on Requirements

The Drafting Team did the best we could laying out levels we know today.

Member Comments

- Focus on the importance of connectivity.
- We need to evaluate - the appropriate format, vs. assuming we will keep the same format. This may be an issue to take up further into to the development of the CIP 002 Standard.

C. Phase 2/Version 3 Working Paper Discussion - Day Two

1. Day One Summary

On Day two the facilitators reviewed the following SDT areas of possible agreement with Working Paper approach and concepts from the day one SDT discussion:

- Recognize different audiences: develop Executive Overview (e.g. will have to protect more assets than before; will require identification of more BES assets than did before; will require different levels of protection) that clarify the intent at a high level regarding methodology;

- Address structured and unstructured threats;
- Develop graphic and tabular depictions of key concepts in white paper;
- Terms and definitions - take a step back and address in content sections;
- Address connectivity as an important concept;
- Seek outside assistance from operating and planning committees for identifying and categorizing BES sub systems and reliability function; and
- Categorize the cyber systems.

The facilitators noted there were several outstanding issues raised by the Working Paper issues and the day-one discussion which could be taken up in small group discussions.

2. 3rd Party Review and Risk Based Approach

The facilitators first reviewed the day one discussion on the section, “3rd Party Review of BES Subsystem Categorization Options” and the related point of consensus from the April 2009 SDT meeting upon which the drafting team had drafted this section which stated: “The Standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES.” The facilitators then reviewed several possible oversight options from the day one discussion including:

- White Paper option - hierarchal structure (entities, reliability coordinator, regional entity and ERO) area wide perspective, entities categorize BES subsystems with oversight by RC, RE and ERO and with burden on reviewer to justify adding to the entities list of categorized BES subsystems and an appeals process.
- Regional Entities develop criteria for categorization of BES subsystems through regional standards development process and ERO review and approval.
- BES System Categorization criteria will be established at the Interconnect wide level and SDT drafts the criteria and augment with subject matter expertise with oversight through the normal audit process.
- BES System Categorization minimum criteria established at the continental level and SDT drafts the criteria and augment with subject matter expertise with oversight through the normal audit process with an option for interconnections to argue for variation or additional more stringent criteria.

The SDT discussed the working paper section on Risk Based Approach to Security Control Selection. Members suggested the needs for some level of flexibility given that this is an exercise in reducing the risk.

SDT Comments on the Risk Based Approach

- Give entity some level of flexibility other than just the TFE – propose a move to a performance based security assessment – write controls to address risk to the asset – valuable based assessment

- Rewriting the requirements and decoupling them from the controls – different types of controls to address requirements – look at environment and have options to address
- Changing the requirements to better point to the controls – with different ways to mitigate the risk
- How do we do what we feel needs to be done within the bounds of the NERC requirements – what a properly written requirement or standard is still a question – these standards are different but can not throw out the auditing system – still have to play within those confines
- Categorizing according to risk impact
- Vulnerability is easier to figure out than threat
- Remember that audits will be to the requirement
- Control based audits work in certain contexts to work out conflicts – that is not how NERC audits – need to write requirements to meet NERC audits
- Gaining consensus on a control based audit system – need to get NERC staff (legal, standards development and audit) on board
- Need to write what the objective is into the working paper to open dialogue with NERC staff
- This aligns with the industry – performance based auditing – sets basis for standards to evolve over time, for lessons to fold back into the standards – this is a culture shift
- Don't agree that the audit system can give much back – because of the way the penalties are assessed

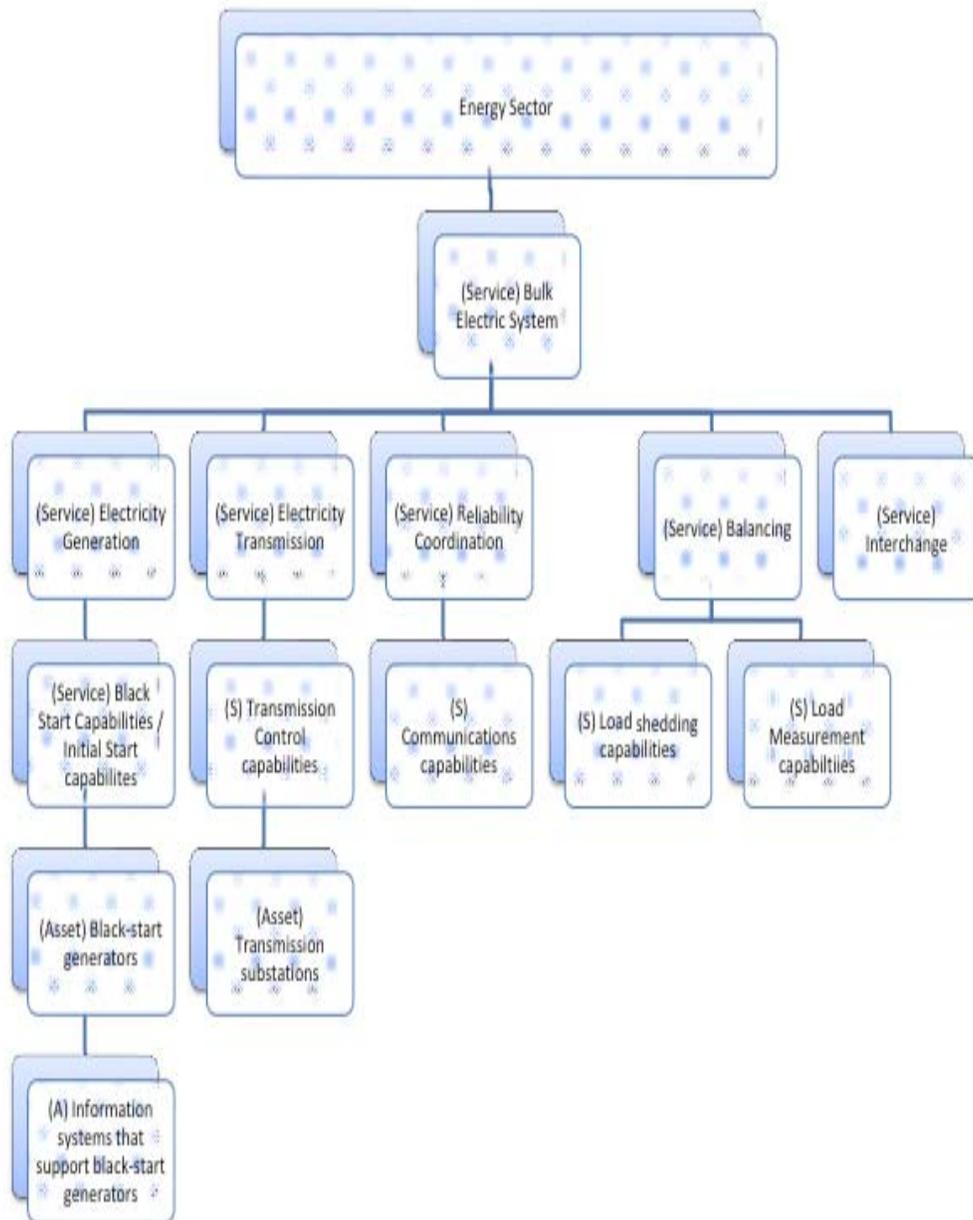
3. Identification of Essential Systems and Categorization of BES Subsystems.

After some clarifying discussion regarding the intent of the white paper, the drafting team agreed to refine the existing section and clarify to what degree the entity should have the discretion to categorize any of the BES subsystems. Of the areas of concern the facilitators identified from day one's discussion, the SDT agreed to work in two small groups to further explore and refine the issues and options.

a. Identification of Essential Systems

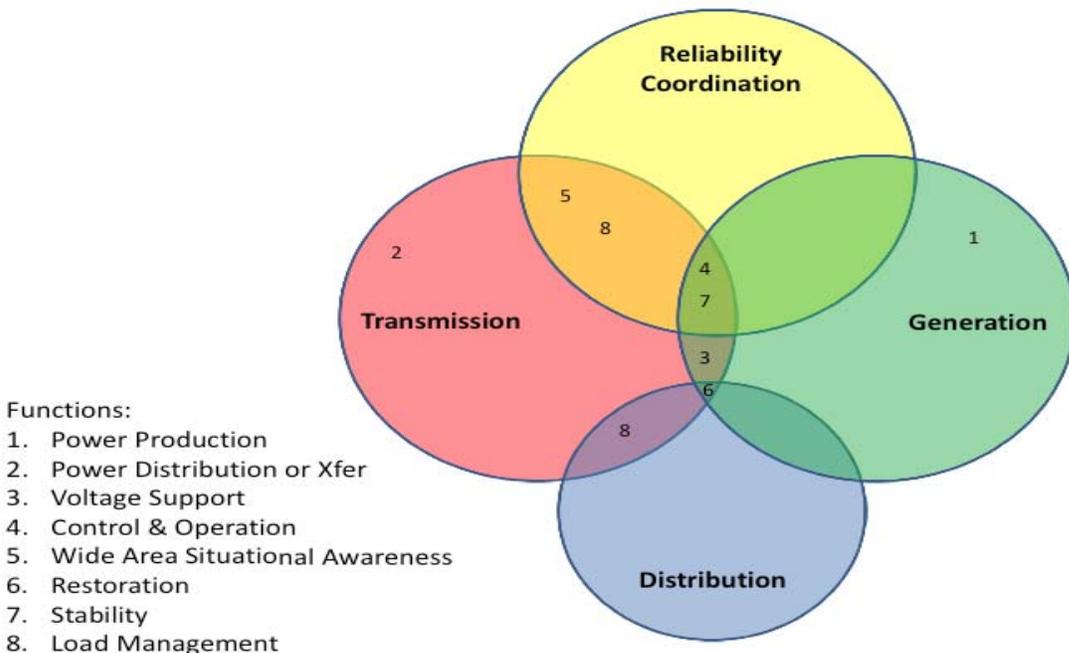
Frank Kim provided a summary of the small group take away points including:

- Reduce ambiguity about what is and is not within the scope;
- Clarify what is meant or included in “other” – list what was meant as examples for the industry; and
- Whether or not integrity of data as to communications is a requirement – integrity of function of the links between systems.



b. Categorization of BES subsystems

Jackie Collett presented the small group’s report using the chart below. She noted they have attempted to graphically relate the eight functions (set out in the working paper) to some of the services – roles. They may try to put in some specific examples for clarity for the industry. Once they flesh this out we can ask committees for their thoughts and reactions. They deliberately tried not to use some of the common NERC terms and they are getting away from who owns it. This will be is an iterative process, a series of steps. The current CIP standards are system – based but you may not be protecting what you really need to protect for purposes of reliability – this is a more holistic approach to what you need to protect. While you may have to protect a thing, it is a collection of things that must operate together. Assessments help compartmentalize what you need to look at – those who claim to not have anything may actually have assets that need to be protected. We will be trying to identify the set of controls needed to protect an asset. In the end the objective will be to come up with categorized list – categorized by level of risk. How can we quantify the impact without knowing its impact on the BES? Most entities currently do not know the impact. We need to set criteria to establish the impact. What is missing now is protecting cyber system and functions – current CIPs do not get us there. The process we come up will need to be agreed to and understood by the industry. We want to apply a consistent level of control – not everything should be protected at high – if filtered through the right criteria – that is the key. We must make sure everyone has a minimum level of protection. Smaller entities need to be made aware of their impact on the larger system. We will have to resolve the issue of market sensitive data.



SDT Comments on the Report

- Still concerned about process of applying everything and categorizing BES stuff – subject to penalties, but have we protected anything?
- Role intended to replays subsystem? No, it is something different
- What is generation? Staying away from it because it means different things to different people
- Question regarding the second column
- Did not consider the question the criteria but rather the level of criticality to the system
- Intent of paper to address the system in terms of functions to get to integrity of the data – address in cyber system interconnections
- Some in industry may be looking for a list – call out some items
- For BES we may offer some examples, not a list – do not want to end up with a check list – reluctant to do so this early – illustrative examples only
- Trying to identify where a system or function fits – examples may help clarify
- EMS is critical because of what it can affect – not critical itself
- Also question of ownership

4. FERC Conference Call and the TFE

Another small group (including Team Members Jeri Domingo Brewer, Kevin Perry, John Lim and Gerry Freese and David Norton and NERC staff) participated in a phone conference with FERC staff regarding the pending interpretation requests for the CIP standards requirements including the including the six wall boundary issues. The SDT members brought up the issue of the currently proposed TFE process limiting TFE requests to only those requirements where technical feasibility was specifically referenced in the standard requirement. FERC staff indicated it was never their intent to limit TFE requests in that fashion and that FERC staff would get with NERC to discuss this further. FERC noted its intent was only to sever the relationship between TFE requests and Reasonable Business Judgment and that they actually intended to broaden the applicability of the TFE request, not narrow it. FERC, NERC and the SDT small group will participate in a follow up call on June 2.

D. SDT CIP Version 3/Phase 2 Process Going Forward

1. Focusing on CIP 002 and Deferring Decisions on CIP 003-009?

The SDT discussed how or whether we need to stay within the current framework of CIP 2-9. Some believe the SDT needs to nail down the broad scope of 002 before having that discussion. The working paper is trying to capture conceptually our expected approach – may need to rephrase how we will go about modeling the existing 002-009. Perhaps the SDT can discuss the expectations about this at an upcoming meeting.

2. Seeking Expert Assistance

The Planning and Operating Committees cannot nominate anyone until June, 2009. The SDT discussed whether it might solicit the informal input of a few individuals respected in the industry. This would not be a substitute for the ongoing participation and contributions of those participating at the meetings and on the WebEx, nor the outreach to the Operating and Planning Committees, nor the briefing of the NERC Members Representative Committee. Several names were mentioned in the SDT conversation and staff agreed to coordinate with member in making the contacts and requests.

3. Concept/Working Paper Readiness for Industry Review, Level of Detail and Audience

The concept for the working paper is to put forward an approach to 002 initially and later fleshing out the detail after getting industry reactions. Many expressed concerns with the level of detail for this working paper and suggested it be more conceptual at this point.

- Use the executive summary to explain the concept without the detail in the rest of the document – the high level overview you want others to review – will not overwhelm others with the detail
- Higher level paper to send out – can not have high level in one section and more detail in others – more detail we put out the more reaction – comments we will get back
- BES continue to put out the system approach to explain change from current system
- Would have to pull back some of the details in the paper today – some of the details go to how to redraft the standards – people already talking about the paper and members are getting questions on details.
- There may need to split into two documents with a summary for the larger body and the detailed version for our use. However care should be taken in splitting the paper into two – the SDT needs input from key individuals with the qualifications necessary to look at both sides

4. Expectations for Adoption of 002

- Multiple rounds of drafts will be needed before we gain consensus with industry – should be parallel to development of standards and controls – if consensus on 002 occurs first then move to ballot but if takes longer than securities control then we may wait and issue together.
- Some prefer putting it out as a whole – less need to put out first if FERC will address TFE interpretation with NERC
- I also agree with waiting till everything is ready – but the SDT and NERC must keep industry updated with drafts – not comfortable voting without the whole package.
- This can remain an open question as needed.

VI. NEXT STEPS

A. 2009 SDT Workplan Approach

Bob Jones, SDT facilitator, noted the proposal to proceed with CIP 002's development in the remaining half of 2009 and refine it after a sequence of comments from the industry before going to the ballot.

B. Workplan Schedule

The Chair reminded people to register for the Portland Bonneville Power meeting and that the July meeting would take place in Vancouver, B.C., Canada.

C. CIP 002 Working Paper Development

The drafting team agreed to continue working on refining the working paper including taking a more conceptual approach while holding the details for consideration as the SDT begins development of the CIP 002. Categorization of the BES assets still needs refinement and help from outside experts. Scott Mix will take the lead to see if additional expertise can be provided to the sub team.

D. Process Evaluation - What has Worked, What could be Improved?

Hal Beardall reviewed with the SDT the results of the process survey undertaken in March and April. (See Appendix #7). Following the review, Stu Langton led a onsite meeting evaluation discussion and members completed written evaluation forms (See, Appendix #3)

The meeting concluded by the SDT members thanking the Chair for her hosting and for the very productive meeting and informative field trip.

The SDT adjourned at 3:45 p.m. on May 14.

Appendix # 1
Cyber Security Order 706 SDT — Project 2008-06
Draft Meeting Agenda

May 13, 2009 | 8:00 a.m. to 3:00 p.m. EDT

May 14, 2009 | 8:00 a.m. to 5:00 p.m. EDT

Bureau of Reclamation
Boulder City, NV

Proposed Meeting Objectives/Outcomes

- Receive update Phase I Recirculation Ballot results
- Review MRC presentation and input
- Receive update on TFE and VSL processes;
- Receive update on the SDT “Key Messages Task Group”
- Review, refine and adopt the Phase II White Paper as a conceptual framework going forward;
- Agree on next steps in the Work plan and assignments.

Draft Agenda

Wednesday May 13, 2009

- 8:00 a.m. Welcome and Opening Remarks- *Jeri Domingo-Brewer/Kevin Perry*
- a. Roll Call
 - b. NERC Antitrust Compliance Guidelines
 - c. Facilitator review of April meeting summary and adoption
 - d. Update on SDT Team Membership
- 8:20 a.m. Review of Meeting Objectives, Agenda and Meeting Guidelines- *Jeri Domingo Brewer and Bob Jones*
- 8:25 a.m. Update on the Phase 1 Recirculation Ballot Results-*Jeri Domingo Brewer*
- 8:30 a.m. Update on NERC Member Representative Committee May 5, 2009 Presentation
- 8:40 a.m. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting-
Scott Mix
- 8:45 a.m. Update on VSLs/VSRs - *David Taylor*
- 8:50 a.m. Update on the “Key Messages” Task Group - *Gerry Freese*
- 9:20 a.m. Overview of FERC Order and Steps to Date in the SDT Phase II Development Process-
Stu Langton
- 9:30 a.m. Phase II Concept Paper Presentation and Discussion- John Lim, Phil Huff, et al
- 10:30 a.m. Break
- 10:30 a.m. Phase II Concept Paper Presentation, Discussion and Refinements- John Lim, Phil Huff, et al
- 12:00 p.m. Working Lunch (Return to plenary meeting at 12:45)

- 12:45 p.m. Phase II Concept Paper Discussion
 2:50 p.m. Drafting Assignments for Thursday
- 3:00 p.m. Recess (Field Trip to Hoover Dam)
- Thursday May 14, 2009** (As revised May 14, 8:00 a.m.)
- 8:00 a.m. Welcome and Agenda Review and Review of Portland Logistics
 8:05 a.m. “Key Issues” Communications Task Group Discussion and Next Steps - Gerry Freese
 8:20 a.m. Phase II Concept Paper Discussion
 Review of SDT Areas of Agreement with White Paper Approach and Concepts-Day One
- Recognize different audiences: develop Executive Overview (e.g. will have to protect more assets than before; will require identification of more BES assets than did before; will require different levels of protection) that clarify the intent at a high level regarding methodology.
 - Address structured and unstructured threats
 - Develop graphic and tabular depictions of key concepts in white paper.
 - Terms and definitions - take a step back and address in content sections
 - Address connectivity as an important concept
 - Seek outside assistance from operating and planning committees for identifying and categorizing BES sub systems and reliability functions
 - Categorization of Cyber systems
- Outstanding White Paper Issues
 3rd Party Review of BES Subsystem Categorization Options (pros-cons and ranking)
 Identification of Essential Cyber Systems
 Risk Based Approach to Security Control Selection
 Final categorization of cyber systems based on overall impact on the BES
- 8:45 a.m. 3rd Party Review of BES Subsystem Categorization Options (pros/cons and ranking)
- 10:30 a.m. Break
- 10:45 a.m. Phase II Concept Paper- Small Group Discussion
- Identification of Essential Cyber Systems
 - Risk Based Approach to Security Control Selection
 - Final categorization of cyber systems based on overall impact on the BES
- 12:15 p.m. Working Lunch
- 12:45 p.m. Phase II Small Group Reports
 2:00 p.m. Clarification of Next Steps on White Paper Development
 White Paper Development and Release - input on BES from Operating and Planning Committees.
- 2:15 p.m. Break

- 2:30 p.m. Work plan and Schedule Issues
- TFE and the SDT - weighing the value and costs of the SDT addressing TFE in 2009
 - CIP 002 - Review and Test Consensus on Developing CIP 002 for Industry Comment and Ballot
- 3:25 p.m. Review of SDT Member Process Evaluation and Steps Forward
- 4:00 p.m. Other Issues
- 4:30 p.m. Assignments, Next Steps and Review of Work-plan and June meeting objectives
- 4:45 p.m. Meeting Evaluation – What was accomplished? What helped? What can be improved?
- 5:00 p.m. Adjourn

Appendix # 2
Cyber Security for Order 706 Standard Drafting Team and Attendees List
May 13-14, 2009 Project 2008-06 — CS 706 SDT

Orlando, Florida

Attending in Person – SDT Members

| | |
|--------------------------------------|--|
| 1. Rob Antonishen | Ontario Power Generation (Tuesday and Wednesday) |
| 2. Jim Breton | ERCOT |
| 3. Jeri Domingo-Brewer, Chair | U.S. Bureau of Reclamation |
| 4. Jackie Collett | Manitoba Hydro |
| 5. Scott Fixmer | Senior Security Analyst Exelon Corporate Security, Exelon Corp. |
| 6. Gerald S. Freese | Director, Enterprise Information Security America Electric Power |
| 7. Phillip Huff | Arkansas Electric Coop Corporation |
| 8. John Lim | CISSP, Department Manager, Consolidated Edison Co.NY |
| 9. Frank Kim | Ontario Hydro |
| 10. David Norton | Policy Consultant, CIPEnergy Coporation (<i>Tues & Wed.</i>) |
| 11. Kevin B. Perry, Vice Ch. | Director, IT-Infrastructure, Southwest Power Pool |
| 12. David S. Revill | Georgia Transmission Corporation |
| 13. Scott Rosenberger | Luminant Energy |
| 14. Kevin Sherlin | Sacramento Municipal Utility District |
| 15. Jonathan Stanford | Bonneville Power Administration |
| 16. Keith Stouffer | National Institute of Standards & Technology |
| 17. John D. Varnell | Technology Director, Tenaska Power Services Co. |
| 18. William Winters | Arizona Public Service, Inc. |

| | |
|--------------------|---|
| 1. Roger Lampilla | NERC |
| 2. Mike Assante | NERC (Wednesday) |
| 3. David Taylor | NERC (Wednesday) |
| 4. Scott R. Mix | NERC |
| 5. Tom Hoffstetter | NERC (Formerly Midwest ISO, Inc) |
| 6. Joe Bucciero | NERC/Bucciero Assoc. |
| 7. Robert Jones | FSU/FCRC Consensus Center (Wed. & Thursday) |
| 8. Stuart Langton | FSU/FCRC Consensus Center |
| 9. Hal Beardall | FSU/FCRC Consensus Center |

SDT Members Attending via WebEx-Phone

| | |
|---------------------------|--|
| 19. Joe Doetzl | Manager, Information Security, Kansas City Power & Light Co. |
| 20. Richard Kinan | Orlando Utilities Commission (Wednesday) |
| 21. Christopher A. Peters | ICF International |

SDT Members Unable to Attend

| | |
|-------------------|---|
| 1. Jay S. Cribb | Information Security Analyst, Southern Company Services, Inc. |
| 2. Sharon Edwards | Duke Energy |

Others Attending in Person

| | |
|-------------|------|
| Bob Tallman | E.ON |
|-------------|------|

Others Attending via WebEx-Phone

| | |
|--------------|--|
| Chris Wright | |
|--------------|--|

| | |
|----------------|-------------|
| Sam Morrell | CERT |
| James Bassett | Lafayette |
| Jason Marshall | Midwest ISO |
| Chris Wright | Burns & Mac |

Appendix # 3 Meeting Evaluation Feedback

CYBER SECURITY ORDER 706 SDT
MAY 13-14, 2009, BOULDER CITY, NV
MEETING EVALUATION FEEDBACK

Members used the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree. The ranks reflect the average for each category statement.

1. Please assess the overall meeting.

8.29 The agenda packet was very useful.

8.71 The pre-meeting papers (White Paper and Process Evaluation Summary) were very useful.

6.17 The WebEx document display and the audio were effective

7.06 The quality of the meeting facility was good.

8.88 The objectives for the meeting were stated at the outset.

8.00 Overall, the objectives of the meeting were fully achieved.

Were each of the following meeting objectives fully achieved:

9.13 Receive update Phase I Recirculation Ballot results

8.06 Review MRC presentation and input

8.31 Receive update on TFE and VSL processes;

7.19 Receive update on the SDT “Key Messages Task Group”

8.12 Review, refine and adopt the Phase II White Paper as a conceptual framework going forward.

8.31 Agree on next steps in the Work plan and assignments.

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

8.33 The Chair and Vice Chair provided leadership and direction to Team and Facilitators

8.76 The Facilitators made sure the concerns of all members were heard.

8.29 The Facilitators helped clarify and summarize issues.

8.29 The Facilitators helped members build consensus.

8.29 The Facilitators made sure the concerns of all participants were heard.

8.41 The Facilitators helped us arrange our time well.

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

8.59 Overall, I am very satisfied with the results of the meeting.

8.65 Overall, the design of the meeting agenda was effective.

8.44 I was very satisfied with the services provided by the Facilitators.

8.50 I am satisfied with the outcome of the meeting.

8.60 I know what the next steps following this meeting will be.

8.00 I know who is responsible for the next steps.

4. Other comments:

What did we achieve?

- Some progress on concept paper

- Consensus on WP
- Improving consensus
- We are getting consensus on the direction the group wants to go
- We obtained a significant amount of consensus on our next steps forward. We needed a lot of direction in the working paper and I think this was achieved.
- We have a course of action that should when complete provide a substantive improvement to electric sector security.
- Major progress on the working paper
- Jon did a good job of summarizing the key points of consensus
- Need for the Key Messages” task group seems to have dissipated.

What are our biggest challenges going forward?

- Keeping to agreed consensus items
- Not getting sidetracked. Keep us on goal!
- After we figure it out...selling it to the industry who did not go through the process.
- Getting industry to agree to this direction
- A lot of work left to do. We need to stay on task
- Industry consensus
- Consensus, industries education
- Time

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

- Better internet access
- Provide copies of all documents prior to meeting
- Small groups remain productive

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 subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

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

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and

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

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

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

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

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

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

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

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

Appendix # 5
CYBER SECURITY ORDER 706 SDT JANUARY- DECEMBER DRAFT PROJECT
SCHEDULE (REVISED MAY, 2009)

OVERVIEW

- **13 SDT FACE-TO-FACE MEETINGS**
- **MULTIPLE SDT SUBGROUP AND SUBCOMMITTEES WEBEX MEETINGS**
- **2 NERC MEMBERS REPRESENTATIVE COMMITTEE MEETINGS, (MAY & AUGUST, 2009)**

CYBER SECURITY ORDER 706 SDT DRAFT SCHEDULE
JANUARY-DECEMBER, 2009

DEVELOPMENT OF CIP FRAMEWORK JAN-JUNE, 2009

1. January 7-9 SDT Meeting, Phoenix, AZ ½ / 1½ day format. Wed-Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products - Establish and convene small groups to draft responses
- Review of Phase 2 White papers
January 15 WebEx meeting(s)
- Small group draft responses to industry.
January 21 WebEx meeting(s)
- Small group draft responses to industry.

2. February 2-4 SDT Meeting, 2009, Phoenix, AZ, ½ / 1½ day format. Mon -Wed.

- Update on NERC Technical Feasibility Exceptions process
- Review of VSL process and SDT role
- Review of Phase 2 White papers, straw man and principles
- Review and Adoption of SDT Responses to Industry Comments on Phase I and Phase I Product Revisions.

3. February 18-19, SDT Meeting, Fairfax, VA

- Update on Phase I process
- Update on NERC TFE process
- Update on VSL Team process
- Review, discussion and refinement of Phase II/CIP 002 White papers, straw man and principles

4. March 10-11, SDT Meeting 2009, Orlando, FL, ½ /1/1 day format

- Update on NERC TFE process
- Update on VSL Team process
- Review and Refinement of Phase II CIP 002 Straw man Proposals

March 2 - April 1 30-day Pre Ballot

Mid-March - NERC posts TFE draft Rules of Procedure for industry comment

March 30, WebEx meeting(s) White Paper Drafting Team

April 1-10, NERC Balloting on Phase 1 Products

April 6, WebEx meeting- White Paper Drafting Team

April 8, WebEx meeting(s) - White Paper Preview- Full SDT Conference Call

April 11, 2009 Phase I Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-

5. April 14-16, SDT Meeting, Charlotte NC, ½ / 1½ day format. Wed-Friday

- Update on NERC TFE process
- Update on VSL Team process
- Update on the NERC Critical Assets Survey
- Agree and Adopt Responses for Phase I Industry Comments- Recirculation Ballot
- Review and Refinement of Phase II Whitepaper and Progress Report to MRC

April 28 and May 6 White Paper Drafting Team Meetings - WebEx.

April 17-27 Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009, NERC Member Representative Committee Meeting, Arlington, VA- SDT progress report.

6. May 13-14, Wed.-Thursday, SDT Meeting, Boulder City NV, 2-day format

- Review MRC presentation and any input to SDT on Phase II approach
- Further SDT refinement of the Phase II White Paper.

CIP 002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JUNE-DEC 2009

7. June 17-18, SDT Meeting, Portland OR, 2-day format

- Further SDT refinement and adoption of the Draft Phase II White Paper.
- Review implementation plan for June-December CIP 002- potential SDT subcommittee structure and deliverables.
- Agree on and charge subcommittees and conduct subcommittee organizational meetings

8. July 13-14, 2009 SDT Meeting, Vancouver, B.C., Canada

- SDT Subcommittees meet to organize and begin drafting revisions to CIP 002 and/or addressing assigned issues.
- SDT Plenary and Subcommittee meetings to review and respond to any industry input/comments on white paper.
- Subcommittee organizational reports to SDT
July-August, WebEx meeting(s)
- SDT Subcommittee meetings as needed

9. August 20-21, 2009, Chicago IL

- SDT Plenary and Subcommittee meetings to develop and test support for CIP 002 products

August, 2009, **NERC Member Representative Committee**, Progress Report presentation on CIP 002 for MRC input, Winnipeg, Manitoba

10. September 9-10, 2009 Folsom, CA

- SDT Plenary review industry and MRC input on CIP 002 approach and consider and agree on refinements
- SDT Subcommittee drafting meetings- requirements etc.
- SDT Plenary Session(s)- briefings and subcommittee reports
- Review Work plan through Summer, 2010, as needed

September, WebEx meeting

- SDT Subcommittee drafting meetings

11. October 20-22, New Orleans LA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s) - briefings and subcommittee reports on CIP 002 Requirements, etc.
- Adopt Work-plan through Summer, 2010, as needed

October, WebEx meeting

- SDT Subcommittee drafting meetings

12. November 17-18, Atlanta GA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s) - briefings and subcommittee reports on CIP 002 requirements, etc.

November, WebEx meeting

- SDT Subcommittee drafting meetings

13. December 15-17, Tampa

- SDT Plenary Session(s) to review, refine and agree on Draft CIP 002 Initial post for industry review and comments
- SDT Subcommittee drafting meetings

December, WebEx meeting

- SDT Subcommittee meetings

SDT 706- 2010

- CIP 002- SDT Respond to Industry Comments, Refine CIP 002
- Initiate CIP 003-009 Development of Requirements, Measures, and Controls etc.
- Develop a full set of CIP 002-009 Standards for Industry Comment

- Refine and Submit for Industry Ballot
- NERC Board of Trustees Adopts
- FERC Approves and NERC Implements

Appendix # 6 Phase II Working Paper

Download the paper at http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706
05/09/2009

Appendix # 7 SDT Process Survey and Recommendations

TO: SDT 706 Team Members

FROM: Jeri Domingo Brewer, Chair and Kevin Perry, Vice Chair, SDT 706.

RE: SDT 706 DRAFT PROCESS SUGGESTIONS GOING FORWARD

DATE: May 11, 2009

Thanks again to the members who provided their thoughts and reflections on the online SDT process survey that our facilitators produced. Your responses underscore the Team's commitment to practical improvements that help us to seek to continue to improve our productivity as a team. Attached to this memo is an executive summary and the complete results (*without attribution but with respondents listed*) of the survey for your information.

Below are our thoughts and reflections based on your responses. We have organized these in 7 areas with suggestions on how we might respond to the survey results and institute practical improvements. We plan to discuss these suggestions at our upcoming meeting with an eye towards implementing those the Team believes will be helpful going forward.

1. SEEK GREATER EFFICIENCY IN OPEN SDT DISCUSSIONS

- SDT members should continue to share the airtime and keep their points brief and well focused.
- SDT facilitators should clarify the objectives of sessions at the outset and manage discussions to achieve those objectives. Use of the "parking lot" tool should be used to keep the SDT on track and bring back off-topic points.

2. USE OF WEBEX AND PHONE-AUDIO FOR SDT MEETINGS

- In planning for meetings, take into account the quality of the facilities' telephone, audio web connections. This is important for the Team members and for others following the SDT process.
- Facilitators should use WebEx to engage members who are participating by phone and ensure that meeting participants voices are clearly captured

3. USE OF SDT SUB-GROUPS TO DRAFT PHASE I STANDARDS (OCTOBER-NOVEMBER, JANUARY-FEBRUARY)

- Subgroups have and will continue to be critical to making progress with the SDT given its size and the complexity of the charge.
- Greater care should be taken in charging the subgroups with clear objectives and consistent formats and consistent definitions of terms to guide their efforts.

- Provide sufficient time for reporting back and agreement for suggestions for further refinements and consensus building.
- Continue to use small groups for drafting responses to industry comments.
- When possible, develop a draft straw man of responses that are consistent and can be refined through the SDT small and full group review and discussion.

4. USE OF STRAWMAN DRAFTS

- Straw man drafts have been effective ways to engage the SDT but multiple, competing straw man documents require more time and effort.

5. USE OF A 4-POINT ACCEPTABILITY SCALE TO PROVIDE A GAUGE OF SDT SUPPORT FOR PROPOSALS

- Facilitators should make sure the SDT is clear on draft conceptual proposals prior to using the ranking tool to test acceptability. It should be used for flushing out divergent perspectives and seeking to find common ground.

6. DISTRIBUTION OF TIMED AGENDAS AND MEETING OBJECTIVES IN ADVANCE OF SDT MEETINGS AND DETAILED MEETING SUMMARIES INCLUDING EXECUTIVE SUMMARIES AND APPENDICES.

- Continue to produce and circulate agendas with objectives
- Facilitators should be clear and explicit with the SDT when the discussion is off the agenda. When the time allotted for the discussion needs adjustment the facilitators should clarify the tradeoffs and make a proposal to chair and team.
- Make summaries available on website and let the members know and give them the precise link where they can draw it down.

7. USE OF ONSITE MEETING EVALUATION

- Use a combination of a group onsite evaluation and an individual evaluation form. Capture and summarize in the meeting summary.
- Facilitators should encourage members to provide informal side-bar feedback on process concerns that can be shared with the Chair-Vice Chair for consideration.

**Cyber Security Order 706 Standard Drafting Team
 On-Line Process Evaluation Survey Results (19 of 23 members)**

EXECUTIVE SUMMARY

(May 12, 2009)

HOW SATISFIED ARE YOU WITH THE PROGRESS THE SDT HAS MADE AND OUTCOMES IT HAS ACHIEVED SINCE OCTOBER, 2008?

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 5 | 8 | 5 | 1 | 2.9 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

STRENGTHS

- Productive group in spite of size
- The breadth of knowledge and experience of team members
- The independent facilitation team allows Team to focus on content
- Phase I was very successful

CHALLENGES

- Managing time effectively
- Managing external issues and pressures - Smart Grid, legislative proposals,
- Managing the impact on the SDT deliberation of high profile issue with lots of media attention.
- Phase II is getting off to a rocky start.
- Balance between discussion and decisions.
- This was a 'fast' process overall. I'd like to be further along with the Phase II ideas
- The development of these standards is complex, and our progress is non-linear.
- It is likely that we won't be able to take a direct path to the result, and will need to wander around. This, at times, may frustrate some team members more than others (and frustrate us all sometimes!).
- The process seems to work, but the progress seems difficult. I expect that once the framework is fully developed, progress will speed up.
- Fear of introducing real security to the electric sector. Given the current environment we need to shift our focus to providing justification and building confidence in the plan we have.

SDT PROCESS ITEMS

(Note: Summary comments are offered for those areas receiving less than 3.0 average)

1. USE OF WEBEX AND PHONE-AUDIO FOR SDT MEETINGS

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 0 | 10 | 8 | 1 | 2.5 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

Summary of Points

- Effectiveness directly proportional to quality of teleconferencing facilities at the face-to-face site. Quality of audio and WebEx has been inconsistent.
- This working is essential to the whole premise of remote participation.
- Participating via phone is very tough to follow. It is usually hard to hear everyone plus when numerous conversations are going on at once you get lost in the noise.
- This has been a combination of process and logistical slip-ups.
- Audio quality seems to be a continuing issue.

2. USE OF WEBEX FOR SUB-TEAM MEETINGS

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 8 | 7 | 2 | 1 | 3.2 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

3. USE OF SDT SUB-GROUPS TO DRAFT PHASE I STANDARDS (OCTOBER-NOVEMBER)

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 9 | 8 | 1 | 1 | 3.3 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

4. USE OF SMALL GROUPS TO DRAFT RESPONSES TO PHASE I (JANUARY-FEBRUARY)

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 8 | 10 | 1 | 0 | 3.4 |
| Totals for | 0 | 2 | 0 | 0 | 3.0 |

5. USE OF STRAWMAN DRAFTS

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 8 | 7 | 3 | 1 | 3.2 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

6. USE OF A 4-POINT ACCEPTABILITY SCALE TO PROVIDE A GAUGE OF SDT SUPPORT FOR PROPOSALS

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 3 | 10 | 4 | 1 | 2.8 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

Summary of Points

- Very helpful - to hear alternate points of view and especially the expectation that dissenters need to provide alternative language and not just vote "no".
- Good mechanism for gauging general group preferences, divergent perspectives and agreements on conceptual approach. Less effective at actually garnering support for a particular approach. Can lead to too much focus on words while missing the idea.
- Need more succinct issues to vote on, or more discussion time up front to more fully flesh out broad ideas.

7. ADOPTION AND USE OF A 75 PERCENT CONSENSUS DECISION RULE WITH A 2/3'S QUORUM

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 8 | 10 | 0 | 0 | 3.4 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

8. DISTRIBUTION OF TIMED AGENDAS AND MEETING OBJECTIVES IN ADVANCE OF SDT MEETINGS

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 9 | 7 | 1 | 0 | 3.5 |
| Totals for | 1 | 1 | 0 | 0 | 3.5 |

9. DETAILED MEETING SUMMARIES INCLUDING EXECUTIVE SUMMARIES AND APPENDICES

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 9 | 8 | 1 | 0 | 3.4 |
| Totals for | 2 | 0 | 0 | 0 | 4.0 |

10. USE OF ONSITE MEETING EVALUATION

| <i>Ranking Scale</i> | <i>Very Satisfied-4</i> | <i>Generally Satisfied-3</i> | <i>Somewhat Satisfied-2</i> | <i>Dissatisfied-1</i> | <i>Avg.</i> |
|----------------------|-------------------------|------------------------------|-----------------------------|-----------------------|-------------|
| Totals for | 3 | 10 | 5 | 0 | 2.9 |
| Totals for | 2 | 0 | 0 | 0 | 4.0 |

Summary of Points

- Some people are in a hurry to leave and may not give the evaluation a lot of thought.
- Comments helpful while they are fresh.
- The process is getting pretty well honed at this point.
- You may get more candid and pragmatic response with a one-on-one sidebar discussion with those that are visibly frustrated during a meeting.
- Evaluations provide an opportunity to address what isn't working