NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

Bonneville Power Administration
Portland, Oregon

June 17, 2009 | 8 a.m. – 5 p.m. PST
June 18, 2009 | 8 a.m. – 5 p.m. PST

Robert Jones 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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Eleventh Meeting Summary,
June 17-18, 2009
Portland, OR

MEETING SUMMARY CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Eleventh Meeting Summary,
June 17-18, 2009
Portland, OR

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer and Vice Chair Kevin Perry welcomed the members at 8:00 a.m. 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 *(See appendix #1*).

Mr. Bucciero reviewed with the Team the need to comply with NERC's Antitrust Guidelines. He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers.

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 reviewed his presentation made a week earlier at the NERC CIPC meeting and noted that NERC staff is now analyzing the comments. NERC staff, including SAIS and outside counsel, is reviewing comments, making responses, and preparing modifications. The NERC BOT will need to approve the resulting TFE document. There is not a requirement for another round of public comments and responses, like the ANSI standards process. The revised TFE will be sent to the Management Representative Committee (MRC) of NERC before being presented to the NERC BOT for adoption. The TFE document will be filed with FERC and will follow the same process for approval as the CIP standards.

Scott also referenced the FERC Order 706 B, which clarified that facilities within each nuclear generation plant in the United States that are not regulated by the NRC are subject to compliance with the eight mandatory Critical Infrastructure Protection (CIP) Reliability Standards, noting that NERC has reconstituted the version 1 SDT and recently convened a town hall meeting that produced a good dialogue and excellent questions.

Scott Mix, on behalf of David Taylor, NERC, also provided an update on the VSL/VRFs. They were posted in May, 2009 for industry comment, and the comment period is now closed. The 93 pages of comments from 10 entities are being reviewed by the respective NERC drafting team. Version 1 & Version 2 VSL/VRFs must be filed by July 1, 2009.

Stu Langton reviewed with the SDT the milestones in Phase 1 and Phase 2 of the SDT work. The working paper has provided a basis for developing the consensus points the SDT agreed to at its Charlotte meeting in April. Joe Bucciero, with the SDT facilitation team, reported that following the Boulder City meeting the Drafting Team has been supplemented with BES expertise from Jim Case,

Jamey Sample, Jack Bernhardsen, Jason Marshall, and Sam Merrill. Others have also been invited to participate, but have not yet done so.

John Lim and Jackie Collett jointly presented the next draft of the Phase 2 Working Paper and invited the SDT to pose clarifying questions, note concerns, and offer options for addressing the concerns. Mr. Lim noted the working paper suggests that this "proposed cyber system categorization" approach includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact-based methodology to categorize the BES subsystems and the associated cyber systems, and finally the deterministic derivation of an overall impact-based categorization of the cyber systems, with the anticipated application of cyber security requirements commensurate with that categorization. This parallels general approaches to risk management practices, which focus first on identifying key processes necessary for meeting high-level objectives, then drilling down into supporting processes.

Jackie Collett noted that the drafting team received help from James Case and Jason Marshall in refining the BES reliability functions and that generation was, in part, revised as a result. The Working Paper Subgroup presented examples of BES subsystems that were intended as simple ways to conceptually illustrate that while the individual impact may be small, it might be big when controlled and is the reason for a high impact determination under common control system. The challenge for the SDT in going forward is developing clear language and criteria when trying to describe these things that can capture the different aspects.

John Lim provided an overview of the current Section on 3rd Party Overview noting that two oversight entities identified in Order 706 - were Reliability Coordinators and Regional Entities. The SDT engaged in a substantial discussion of this section.

The Working Paper Subgroup also presented a new depiction of the"targets of protection" noting that the essential cyber systems don't necessarily stop there. The SDT suggested ways to provide a graphic description without the use of a target metaphor, as was included in the draft Working Paper.

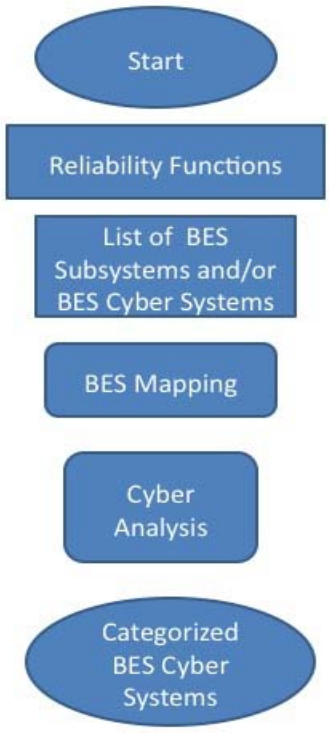
To gain a sense of the SDT and to provide a focus for ongoing SDT discussions, the facilitators asked the members to rate each section of the working paper based on their view of whether the current sections were ready for sharing with the industry (*Are the concepts contained in the working paper sections acceptable for sharing with the industry? 4= Acceptable; 3= Acceptable with minor concerns; 2= Unacceptable unless Address serious concerns; 1=Unacceptable)* Following the rating, the SDT took up a second round of focused comments and suggestions for changes to the seven sections of the document receiving less than a 3.0 average rating. These discussions occurred in the afternoon of June 17 and the morning of June 18 including:

1. 3rd Party Oversight of BES Subsystems Categorization - Review of Concerns (1.9 of 4 Avg.)
2. Defining the Target of Protection (2.5 of 4 Avg.)
3. External Cyber Systems (2.6 of 4 Avg.)
4. Categorization- BES Subsystems, Cyber Systems, and Final Cyber System
   - Categorization of BES Sub-Systems (2.8 of 4 Avg.)
   - Categorization of Cyber Assets (2.8 of 4 Avg.)

- Final Categorization of Cyber System based on Impact to BES (2.5 of 4 Avg.)

5. Identification of Essential Cyber Systems (2.7 of 4 Avg.)

The SDT broke into small groups to discuss and further develop the following scenario concerning the BES Subsystem and Cyber System categorization approach. This led to a further discussion of developing a different sequence for the categorization approach. There was broad SDT member support for this simpler graphic depiction as a working concept for inclusion in the Working Paper.



The SDT Chair, Co-chair, and Members expressed their thanks and appreciation to all those participating on the Working Paper Drafting Subgroup. Before the Vancouver meeting, John Lim agreed to work with Phil Huff, Jackie Collett, and all other interested SDT members to:

- Produce the next draft of the Working Paper, which will be circulated as a final draft for consideration in Vancouver before seeking industry comments.
- Take the review comments of the "target" and produce another graphic using an alternative depiction.
- Continue efforts to develop additional working papers for SDT review going forward on BES Risk Management and Security Controls.

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

The Chair reminded the SDT Team Members that the SDT would try to establish the 2010 meeting schedule at the July SDT meeting in Vancouver, B.C., Canada. For the time being she noted that the August meeting will take place as scheduled in Chicago pending confirmation of available meeting space. *(Note: The venue for the August Meeting was changed to SERC's facilities in Charlotte, NC subsequent to the close of the meeting.)*

Dave Norton advised the group of a call for self-nominations closing on June 25 for a new SAR drafting team which would be defining next generation of situational awareness control tools for the BES.

The Chair (Jeri Domingo-Brewer) thanked Jon Stanford for hosting this meeting at BPA in Portland, Oregon. The Chair also noted the progress made on the draft Working Paper and, in particular, the refining and simplifying of the process flow chart in determining the categorization of cyber systems and BES System assets. The Chair thanked the Working Paper Drafting Subgroup members for an outstanding job. Members completed an onsite meeting evaluation form.

The SDT adjourned at 3:00 p.m. on June 18.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
DRAFT ELEVENTH MEETING SUMMARY,
JUNE 17-18, 2009
PORTLAND, OREGON

I. INTRODUCTIONS, AGENDA REVIEW AND REVIEW OF SDT WORKPLAN

The Chair, Jeri Domingo-Brewer, and Vice Chair Kevin Perry welcomed the SDT members and guests, and called the meeting to order at 8:00 a.m. on June 17th. 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.

II. UPDATES

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

Scott Mix provided an update briefing to the SDT noting that the posting period for the TFE had closed with 52 organizations providing comments over 450 pages. He reviewed his presentation offered a week earlier at the NERC CIPC meeting and noted that NERC staff is now analyzing the comments received on the TFE posting. All comments have been posted on the NERC web site. NERC staff is now reviewing and considering modifications to the TFEs 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 several issues raised in the industry comments including:

- Making TFEs applicable to other standards where there is "triggering language"
- Requirement vs. sub requirement - anything under requirement can be covered by a TFE without change.
- CIP 003 R2.3, and/or CIP 003 R3 - an exception to an internal policy is not a compliance issue since it is not a reliability issue.
- NERC staff is currently cleaning up definitions.
- Economic security - doesn't appear in this section.

- Clarification of the Pre-approval process in terms of review and approval by regions. There will probably be a greater role than in the original posting.

Member Comments

- Has NERC considered issuing a statement on requirements/sub-requirements? The statement should cover all reporting so it is consistent.
- Any reaction from CIPC to CIP 003 R2.3? No reactions to this.
- TFE under new procedure is in effect July 1? However, the TFEs are not approved yet. If the TFE process is not approved before June 30, it is in play? If it is in play, and we have a TFE on the table, can we be held out of compliance? Problem for registered entity, ERO and regional. Self-reports of non-compliance? Bad position based on scheduling, workload.
- Adhere to the spirit of the process? Need to resolve this. Sanctions component may be adjusted in this transition period.
- Does NERC have an alternative plan?
- FERC is aware of issue and plans to discuss with NERC to handle this.
- Escalate the TFE issues to the Commission. Roger Lampila will take a note and check with Mike Assante.
- Single request covering multiple requirements for a covered asset.
- How to submit to multiple regional entities?
- Need to resolve the senior manager language - the senior manager or delegate. Why would it be any different? The company's assigned authorizing officer? Sign off on the TFE.
- Removing automatic 60 days. Maybe NERC has 60 days to extend the request. Won't be an automatic disapproval.
- NERC needs to be timely in its response.
- Mitigation plans go to regional entity.
- Will a TFE disapproval generate a spot-check? Problem is a self-report compliance plan. If you don't, self report a denied TFE. Will that invoke a spot check? Sufficient cause to trigger a spot check. No surprise. Advantage to do as a self-report.
- Canadian entities - self report to whom? To the regional entity? Follows the rules for self-reporting. Agreement in place but different for each province.
- Wide area analysis - not as justification for denying TFE. Rewording with fairness in mind - understanding the impact not necessarily for purpose of denial (maybe the first one, not subsequent ones).
- TFE's need to be dealt with on their technical merit only.
- Anticipate BOT to adopt TFE. When? No sooner than August 4-5. Realistically looking at the November meeting.
- BOT Actions without a meeting? Doesn't apply to this.
- FERC process for acceptance probably 2010.
- Reaction at CIPC? Mostly they understand.
- NERC and the industry are trying to make the best of a bad situation.

Mr. Mix concluded that:

- NERC staff, including SAIS and outside counsel, is reviewing comments, making responses, and preparing modifications. NERC BOT will authorize for adoption. There isn't a requirement for another round of public comment nor a response-by-response submittal like the ANSI standards process. Will pass by the Members Representative Committee (MRC) before presenting to BOT for authorization.
- Will follow the same process for adoption and FERC approval.
- In addition Scott referenced FERC Order 706 B on CIP standards for nuclear. NERC has reconstituted the Cyber Security Version 1 SDT. It has 180 days after issuance of the Order (Sept 15). It has met twice by teleconference and convened a 4-hour town hall meeting. Tim Roxy, Scott Mix, and Gerry Adamski were present from NERC, and Scott Morris with the NRC talked about NRC revisions and noted the newly identified critical asset plan was a good starting point for the implementation plan. Scott also noted the town hall produced a good dialogue and excellent questions

B. Update on VSLs-VRFs

Scott Mix, on behalf of David Taylor, NERC, provided an update on the VSL/VRFs. They were posted in May 2009 for industry comment, and the comment period is now closed. The 93 pages of comment received from 10 entities are being reviewed by the SAR drafting team, and Version 1 & 2 VSLs must be filed by July 1. NERC didn't receive a lot of comments on Version 2.

Member Comments

- Does the NERC BOT have authority to file even if industry rejects the VSLs? Yes, with "extenuating circumstances."

III. SDT PHASE 2/VERSION 3 DEVELOPMENT PROCESS - THE "WORKING PAPER"

A. Overview of Phase 2/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 that framed the challenges, the subsequent development of "white papers" following the Washington D.C. meeting in December, 2008 and further review and refinement of those and other papers. This resulted in the SDT convergence on a single consensus approach in Orlando that was refined further in Charlotte and Boulder City with John Lim, Jackie Collett, and Phil Huff leading an expanded drafting team to continue to refine the draft working paper between meetings. The working paper provided a basis for

developing and testing the following consensus points in April that were subsequently offered to the NERC Members Representative Committee (MRC):

1. The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems.
2. The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.
3. The Standard's BES Impact Assessment will consider a categorization process.
4. 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.
5. The Standards will categorize Cyber Systems supporting, either directly or indirectly, the reliability functions of the BES and apply security requirements (or controls) that are commensurate and appropriate to their potential impact on the BES.
6. The final Cyber System categorization will reflect the impact to the BES based on a loss of availability, integrity, or confidentiality of the Cyber System.
7. The Standards will provide Organizations with reasonable flexibility in applying equivalent security controls on the basis of compensating controls and environmental considerations.
8. The Standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.
9. The Standards will state explicit criteria for the BES Impact Assessment.
10. The Standards will state explicit criteria for the Cyber Impact Assessment (including use and misuse of cyber systems).
11. The Standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.

Joe Bucciero, with the SDT facilitation team, reported that following the Boulder City meeting the Drafting Team has been supplemented with BES expertise from Jim Case, Jamey Sample, Jack Bernhardsen, Jason Marshall, and Sam Merrill. Others have also been invited to participate, but have not yet participated.

B. Phase II Working Paper Overview Presentation and SDT Discussions

On behalf of the SDT, the Chair thanked John Lim, Jackie Collett, Phil Huff, and the other members of the drafting team for working productively since the Boulder City SDT meeting and expressed her gratitude for their leadership and good efforts. John Lim and Jackie Collett jointly presented the working paper (*See Appendix #6).* They noted the expanded team met twice by phone/WebEx following the Boulder City meeting.

1. Overall SDT Comments on Working Paper

The Team engaged in an initial discussion of the working paper as part of the overview presentation. A summary of the SDT member comments are noted below. The presentation

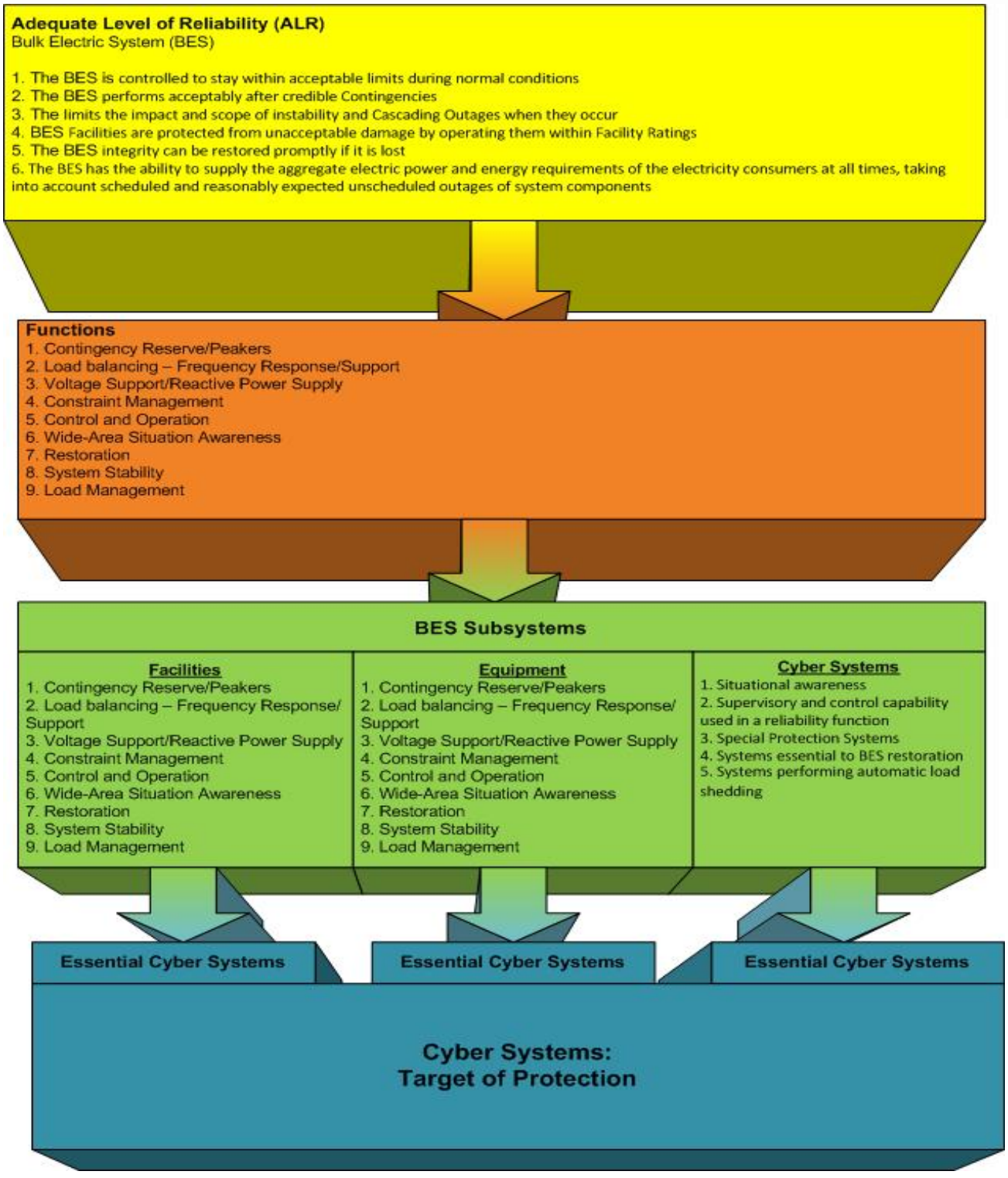
was interactive with the SDT who posed clarifying questions and offered ideas for refinements.

Member Comments- Overview

- The SDT should note that the recent Congressional testimony speaks of dealing with a "sustained cyber attack" which may be different from providing CIP protection.

2. Introduction

John Lim provided an overview for a new chart highlighting BES reliability functions and the conceptual approach the paper is taking in categorizing cyber systems:


Adequate Level of Reliability (ALR)
Bulk Electric System (BES)
1. The BES is controlled to stay within acceptable limits during normal conditions
2. The BES performs acceptably after credible Contingencies
3. The limits the impact and scope of instability and Cascading Outages when they occur
4. BES Facilities are protected from unacceptable damage by operating them within Facility Ratings
5. The BES integrity can be restored promptly if it is lost
6. The BES has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components
Functions
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
BES Subsystems
Facilities
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Equipment
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Cyber Systems
1. Situational awareness
2. Supervisory and control capability used in a reliability function
3. Special Protection Systems
4. Systems essential to BES restoration
5. Systems performing automatic load shedding
Essential Cyber Systems
Essential Cyber Systems
Essential Cyber Systems
Cyber Systems:
Target of Protection

He noted the working paper suggests that this "proposed cyber system categorization approach includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact based methodology to categorize its BES subsystems and the associated cyber systems engaged in the process, and finally the deterministic derivation of an overall impact based categorization of the cyber systems, with the anticipated application of cyber security requirements commensurate with that categorization. This parallels general approaches to risk management practices, which focus first on identifying key processes necessary for meeting high level objectives, then drilling down into supporting processes."

Member Comments on the Chart

- Are the ALR references taken verbatim? Are these words "chiseled in granite"? Change to BES vs. systems. If it meets all of the following characteristics.
- Received some comments on last bullet.
- These are BES reliability functions believed to be necessary to maintain a reliable BES.
- Consider annotating the diagram to illustrate what is meant.
- The Working Paper Drafting Subgroup knew going in this would be more cumbersome than what we have.
- Should we identify the cyber assets first?
- Working Paper Drafting Subgroup presented the concept for reaction
- Identifying cyber assets first may be better in some cases. Whether you do the assets - you are coming back to same list in the end. Perhaps we can provide some flexibility on which way entities may want to go on this?
- Clarify what is the difference/distinction of a cyber impact vs. BES impact? Look at cyber impact in terms of its function and how it fits in BES. Impact of cyber device on BES subsystem.
- Positive side of big picture is that we are signaling we are proposing going in considering both aspects and how they interact to achieve the reliability outcome is important.
- Should the "hard and fast line" of over 500 kV be a minimum baseline?

3. BES Reliability Functions

Jackie Collett noted that the Working Paper Drafting Subgroup received help from James Case and Jason Marshall in refining the BES reliability functions *(pp 11-15 of the Working Paper)* and that generation was, in part, revised as a result.

Member Comments- Overview (**BOB: These are duplicate comments from the previous section above. Is that what you wanted?**)

- "Peakers"? Each will touch on some or multiple components of ALR.
- Are the ALR references taken verbatim? Are these chiseled in granite words? Change to BES vs. systems. If meets all of the following characteristics.
- Consider annotating the diagram to illustrate what is meant in different parts of the chart.

- The Working Paper Drafting Subgroup knew going in this would be more cumbersome than what we have.
- Should we identify the cyber assets first?
- Working Paper Drafting Subgroup presented the concept for reaction
- Identifying cyber assets first may be better in some cases. Whether you do the assets - you are coming back to same list in the end. Perhaps we can provide some flexibility on which way entities may want to go on this?
- Clarify what is the difference/distinction of a cyber impact vs. BES impact? Look at cyber impact in terms of its function and how it fits in BES. Impact of cyber device on BES subsystem.
- Positive side of big picture is that we are signaling we are proposing going in considering both aspects and how they interact to achieve the reliability outcome is important.
- Should the "hard and fast line" of over 500 kV be a minimum baseline?

4. Identification of BES Subsystems

The Working Paper Drafting Subgroup presented examples of BES subsystems that were intended as simple ways to conceptually illustrate that while the individual impact may be small, it might be big when controlled and is the reason for high impact for under common control system. The challenge for the SDT in going forward is developing clear language and criteria when trying to describe these things that can capture the different aspects.

Member Comments

- SDT should be careful - when we talk about "restoration" as people may tune out if they believe reliability is not the issue. Let's try to address these issues with the industry head on.
- In the Final Categorization of Cyber system- Example 1. BES Subsystem A with Relays A, B & C. What changes the BES subsystem impact.

5. Third Party Oversight

John Lim provided an overview of the current section noting that two entities were identified in FERC Order 706 - Reliability Coordinators and Regional Entities. The current draft pointed out that, "Of the 17 Reliability Coordinators in the NERC Compliance Registry, 12 are registered under multiple functions (i.e., BA, TOP, IA, TSP, TP, PC). These 12 RCs could not meet the FERC Order 706 requirement for "external" review for their other registered functions. As an example, Midwest ISO is registered as a RC, BA, PA, and TSP. Midwest ISO RC could not review the list of BES subsystems from the Midwest ISO BA while meeting the FERC requirement for an "external" review. Thus, a third-party review of the third-party review would be required."

Member comments

- RC's oversight authority? Liability and risk in determining whether an asset should have been identified or not.
- Task the RCs to provide guidance. We will need a "safe harbor".
- FRCC - Regional reliability Organization. Member services functions with FRCC - with different committees. Regional organizations that perform functions other than compliance. E.g. FRCC operating committee.
- RCs don't perform reliability function - this is separate function. They have the proper view/ability to have the proper view that REs don't have.
- Is there a conflict of interest for the REs?
- Is there a way to develop this so that you don't need a 3rd party review- because you can agree on the methodology as producing the correct result.
- RE vs. RRO issue: Different interconnections do things differently. Jurisdictional elements - RE is it right now for the new NERC ERO. RROs only exists in the previous "council" world. RROs were never functional models.
- RRO vs RE functionality - different in different areas. Varies on how functions are set up, e.g. differences between Eastern and Western interconnection?
- RC's probably come the closest for surveillance. Need to do it in a "hold harmless" environment.
- Is this an IMPO (???) like function? Technical arbiter. If they are told not to go towards the RCs, they won't go there. Not clear for how industry is overlaid on functional model.
- Conflict of interest with the Regions.
- Create a new kind of arms length entity - serious experts and knowledgeable people. This is not a small thing. No big picture.
- FERC representative, Mr. Peters, indicated that this is a difficult issue. Should be some way for companies to get assistance so they don't get nailed if they get something wrong. There will be conflict of interest on some options. He will be talking with staff and briefing new commissioner coming in soon.
- This implies analysis but how much is not clear. RC to the RE function. Not purely a statutory function. Only because compliance exists that it has to be performed. Is it reliability related? If it is falls under RC. Don't have the capacity currently to provide level of analysis.
- This is based on an electrical system view of the world.
- We need consistency.

6. Identification of Essential Cyber Systems

The Working Paper Drafting Subgroup 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

- What are the key systems we need to put a focus on protecting vs. identifying high/medium/low?
- SDT is okay with the current draft section.

7. Categorization of Cyber Systems

The Working Paper Drafting Subgroup presented an overview of this section noting that:

- The draft is tentative and conceptual.
- The availability and integrity have a bigger impact than confidentiality on the BES.
- Work out how to deal with these further when SDT works on the standards and controls.

Member Comments

- How would a periphery system (AC) be lumped into groups? We will address that when we get to "target of protection" section.
- "Directly" vs. "indirectly"?
- Is this an impact assessment vs. a categorization? How does time factor into this concept? For a minute, hour, day, month a year. Does it factor into high, medium, low. Longer period for availability, shorter for integrity.
- May factor into criteria.

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

The Drafting Team described the concept they are presenting as suggesting you will have finite ways to do this with the end product resulting in the same number. This categorization in turn will determine the selection of the menu of controls.

An example of the application of this approach in an evaluation matrix is shown below:

> **Note:** This table is a visual representation of what the categorization should look like, it's not the actual table.

Asset Impact -->	High	Medium	Low
Cyber Impact:			
High	5	4	3
Medium	4	3	2
Low	3	2	1

The Drafters noted that to the left is the BES system, to the right is the Cyber System, and you merge these to get final categorization.

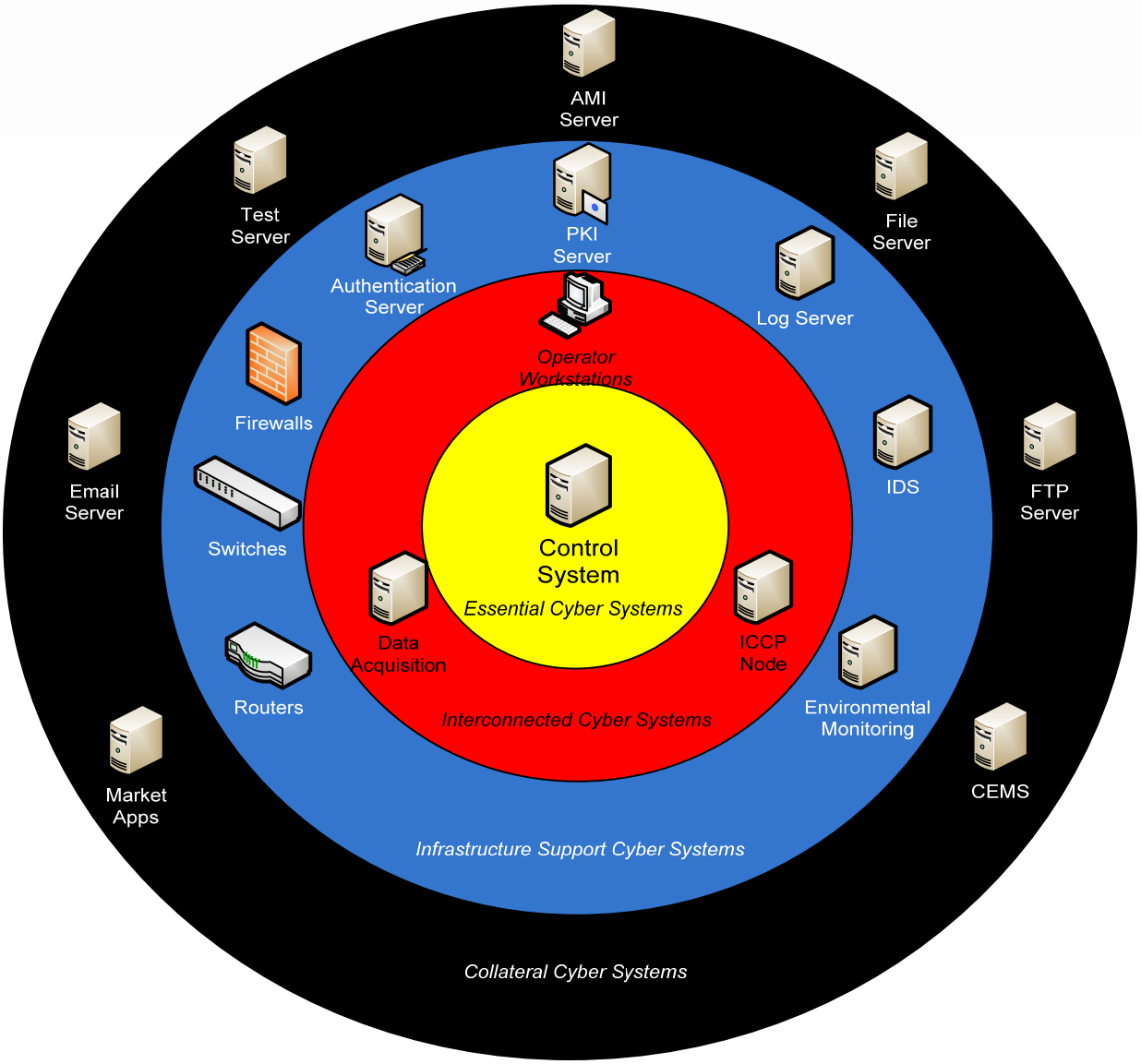
9. Target of Protection

The Drafters noted that the essential systems don't stop there:

1. Essential cyber systems - in middle, e.g. control system
2. Next: Interconnected Cyber Systems, e.g. data acquisition, ICCP node, operator workstation
3. Infrastructure Support Cyber Systems: e.g. switches, routers, firewalls, log service etc.
4. Collateral Cyber Systems: market apps, email server, test server, AMI server, etc.

Comments on Target of Protection

- EMS system in a control center? Fire suppression system and AC control system? Conceptual point is that you must protect them to some level and you can't just ignore. Level of protection depends on impact.
- Environmental monitoring and controls included. Checklist of the things you need to include. Sounds workable.



- AMI systems (smart grid) will be more in the mix going forward. Those may need more protection than collateral cyber systems.
- Market applications and control systems work together in an integrated fashion and may need to be treated together as essential.
- Is there going to be flexibility in this? Don't want the industry to draw the wrong idea from this depiction.
- Market centers playing an increasing role in reliability (nodal). They may need to be in closer to essential. E.g. retail electric provide - way you control and represent your load may make it more essential.
- Address more of these emerging entities.
- "Enabling technology" for perimeter devices and how to protect is an issue.
- Virtual systems coming in - virtual switchers and routers = where do they fit?

- Need to be clear as to what time frame we are focusing on.
- Time frame - CIP does not include planning - real time operation. Worry as well about how it is connected not just when.
- Included because it is a collateral system.
- Not all market operations/functions are day - ahead planning.
- Functions and balancing authorities - how are they treated?
- Ask what is the application doing, and how is that function impacting on the BES? Keep this in mind we may need to locate it in both realms. Real time market control system may belong in essential systems.
- As companies "virtualize" environments, functions become "cloudier." Does the level of protection change because of function or an attack perspective? If they don't perform an essential function, they will be on the collateral list.
- From the perspective of a vertically integrated utility - 8 or 9 BA functions. Who is what, where? What scared Jim Case the most when he was reliability coordinator? "spooks, schedules and tags." E.g. billing is out of this. When put IP on then it changes.
- Salience of market applications - 1 hour in the life of reliability coordinator.
- Who is running email in their control environment?
- Talking first, now, about **what** to protect then later we will get to how to protect it. Shouldn't worry now about how to do this. 1 road leads down reliability requirement another goes another way.
- E.g. OATI - market app to remote platform - used to drive AGC. Not the server, it is the data that is important not the market app unit.
- Got into contract SAS70-2- NERC CIP is in contract will be compliant. Have protection on server.
- Different systems - where is the back to maintain as a critical asset - back up email system to support - costs are significant. Layer of targets and ways we lay application - up to each SCADA engineer - won't be able to categorically say - no two will probably look alike.
- Critical server for business reasons vs. reliability.

10. External Cyber Systems

The Drafting Team provided an overview of this section noting that references to the Interconnection section in the paper. The concept is to put adequate controls to protect the whole system with contractual agreements to protect system to the level needed. The Registered Entity is responsible for protecting cyber systems.

11. Applying Security Controls

The drafting team provided an overview of the section noting that under the current standard you are either in or out, but the application of security controls will allow a greater degree of protection and this would be taken up in the hard work ahead in 2010.

C. Rating the Current Acceptability of the Working Paper Sections following the Overview

To get a sense of the SDT and to provide a focus for ongoing SDT discussions, the facilitators asked the members for rate each section on their view of whether the current sections are ready for sharing with the industry. Following the rating the SDT took up a second round of focused comments in the afternoon of June 17 and the morning of June 18.

Categorization of Cyber Systems Concepts – SDT RATING RESULTS 6-17-09
Are the concepts contained in the working paper sections ready/acceptable for sharing with the industry?
4= Acceptable**; 3**= Acceptable with minor concerns; **2**= Unacceptable unless Address serious concerns; **1**=Unacceptable

	Avg.	4	3	2	1	T
•BES RELIABILITY FUNCTIONS	3.6	11	5	1	0	17
•IDENTIFICATION OF BES SUBSYSTEMS	3.0	2	13	2	0	17
• CATEGORIZATION OF BES SUBSYSTEMS	2.8	1	11	5	0	17
• **THIRD-PARTY OVERSIGHT OF BES SUBSYSTEMS/ CATEGORIZATION**	**1.9**	**0**	**0**	**16**	**1**	17
•IDENTIFICATION OF ESSENTIAL CYBER SYSTEMS	2.7	2	8	7	0	17
•CATEGORIZATION OF CYBER SYSTEMS	2.8	2	9	6	0	17
•EXTERNAL CYBER SYSTEM DEPENDENCIES	2.6	2	7	8	0	17
•FINAL CATEGORIZATION OF CYBER SYSTEM BASED ON OVERALL IMPACT ON THE BES	2.5	4	8	4	1	17
•DEFINING THE TARGET OF PROTECTION	2.5	2	4	**11**	0	17
SECURITY CONTROLS TO THE TARGET OF PROTECTION	3.3	6	10	1	0	17

D. Second Round of SDT Comments on Working Paper

The SDT reviewed on a second round the seven sections of the Working Paper which received less than a 3.0 average rating. Members were asked to describe the concerns that led them to provide a 2 or 1 rating for a section and the SDT discussed possible options for addressing these concerns.

1. 3rd Party Oversight of BES Subsystems Categorization- Review of Concerns

Are the concepts contained in the working paper sections acceptable for sharing with the industry?
4= Acceptable; 3= Acceptable with minor concerns; 2= Unacceptable unless Address serious concerns; 1=Unacceptable

Working Paper Section	*Avg.*	4	3	2	1	*Total*
3rd Party Oversight of BES Subsystems Categorization	**1.9**	**0**	**0**	**16**	**1**	**17**

Member Comments on 3rd Party Oversight Ratings

- Were there any 2 or 1 ratings based on the level of detail? None.
- Do we need this in our concept paper? Should it be removed?
- **Audit vs. Oversight?** Concept of being audited- doesn't that imply 3rd party oversight?
- Does oversight= audit? Audits do play a role in this at an untimely expensive stage in the process.
- Analysis associated with this oversight- point is reliability not compliance.
- Let in the Reliability Coordinator and call it done?
- We need a front loaded process- what do I need to do to get it right going forward. Should not be considered audit function.
- Should we get industry feed back on having the RC do this?
- 706A- rehearing order- FERC- industry sorts out on a contractual basis.
- Voted 1 because of the belief that this section is a non-starter. Issue is fraught with problems and pitfalls. Rather than trying to propose a solution, drop it out or acknowledge and discuss all the problems that have to be overcome in order to do a 3rd party review.
- Discuss the problems vs. a solution.
- This issue is larger than CIP 002- it might be wise to take it out of paper altogether. Consider developing a separate working paper?
- Industry might respond - why don't they tell me what to protect?
- **Quality Control vs. Categorizing Cyber Systems.** Voted 2 because it doesn't fit in terms of concepts trying to communicate to the industry. More of a quality control element vs. a concept about identifying and categorizing cyber systems and assets. FERC in the order was looking directly at version 1`of CIP and its "all or nothing approach." This is a different concept that directs us towards what is most important to protect.
- The drafting group can take the verbiage out and identify there is an issue and will address going forward.
- Concerned this, as drafted, will provide a distraction from the paradigm shift suggested by the broader conceptual approach.
- Criticality level of BES and cyber asset. More impetus for 3rd party overview. Acknowledge to extent "individualism" is taken out of the process, it will be less important for this overview.

- To certain extent- we need more industry input. If we can show them there is a necessity for 3rd party oversight if we go with the old CIP approach, it will be clearer why change is needed. Everyone is responsible for security if you are connected to it. If we go with the new approach, oversight not as big an issue. Anyway we go we have a lot of work to do in this area for both 002 and for the industry.
- If we have a 3rd party analyzing these lists- we will need to provide a whole process for appeals etc. If we could come up with a way that utilities can't use "don't have any critical assets." The current draft calls for an arbitration procedure.
- Mike Assante is taking the lead. This will need to be performed.
- Last thing we want to see is increasing gamesmanship through a new approach. We must get around and place behind us those people trying to keep cyber assets off their list.
- Lots of stuff falls between the cracks. Need to keep coming back to reliability and not compliance.
- Clearly this isn't ready for prime time. Could we reword some of this? Oversight will depend on how it is written- change language- depends on how proscriptive the standards develop.
- That could get some comments from industry as to one approach or the other.
- Somebody will need to take a big picture look at this.
- Sub station - e.g. CIP 002 - task the asset owners. None of the questions focus on ownership vs. operators.
- As a practical matter, is this more bother and trouble that it is worth. Suggest pulling this out and put off to another white paper.
- We should say something but pull the "proposal".
- Question for group- do we strike it totally or do we acknowledge briefing- any issue of wide area overview will be dependent on latitude given to the entity. In favor of getting rid of it outright.
- If a Balancing Authority has the requirement for another entity to protect the other entity assets- occurs in the wide area view? Is there another way to determine?
- Everyone knows that 706 said you need oversight, so we probably have to say something. Even to say, method of oversight doesn't impact on this methodology. Have to say something about "the elephant in the room."
- Reliability considerations- don't use oversight in the paper. Give FERC time to work.
- Note that there are "other issues" in the order that the SDT is not addressing, e.g. BPA's confidentiality issue. Shouldn't place the focus in on this.

At the conclusion of the discussion, the facilitators conducted a straw poll asking members to choose the conceptual approach they preferred for this section:

- Improve it and include as a full section - 0 yes
- Strike it entirely - 10 yes
- Acknowledge in a limited way. 7 yes

The facilitators then tested the support for the following: "Regardless, we should have a group that will continue to look at this issue"–14 yes/2 no

Scott Mix agreed to craft some draft language that there are other considerations in the order that do not directly play into a categorization methodology and will be taken care of at the appropriate time. On June 18, Mr. Mix offered the following sentence to add into the Introduction of the Working Paper:

> "This paper deals only with the identification and classification of BES assets and cyber systems. There are a number of other issues raised in 706 not addressed in this paper. The Team will be soliciting industry feed back on other issues as a part of the CIP standards development process."

Member Comments

- Should be noted as a future consideration
- Focus on task at hand on this paper.
- RK: likes the words. "Dealt with separately"- through additional working paper- will the industry think "secret"
- The team will be soliciting industry feed back at a future date as part of the development process.

6. Defining the Target of Protection

Are the concepts contained in the working paper sections acceptable for sharing with the industry?

4= Acceptable; 3= Acceptable with minor concerns; 2= Unacceptable unless Address serious concerns; 1=Unacceptable

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Defining the Target of Protection	**2.5**	**2**	**4**	**11**	**0**	**17**

Member Comments on Rating and Concerns

- Were there any 2's on the issue of insufficient detail? No
- Gave it a 2. Confused the issue of after categorization of systems - seemed to add a additional piece of complexity. What did it mean in terms of applying controls.
- Any box becoming compromised, becomes easy to compromise every other box. Does this imply there is less protection needed in blue vs. red ring?
- Need to look at the paper and the diagram to understand the intent. Intended to get people trying to think about. Text indicates the sequential of identification vs. relative importance.
- Target of evaluation - common criteria of security mechanisms. Each device in the target has to have a profile for that in terms of high/medium/low.
- We need to make sure it communicates message-i.e. level of importance.

- Could modify showing arrows from center out, with language saying the intent of the sequence of identification?
- The words are there. It is a presentation issue.
- We don't have any substation gear represented? Wouldn't hurt to throw a few in. Lots of people in that world.
- We could come up with another example. PLC control system in the center.
- The graphic reinforces the "control center-centric" perception of the SDT's effort. Have a couple of illustrations: 1 for control center, and 1 with a plant perspective? 2 of the same diagrams with different devices on it.
- Essential cyber assets identification- a cyber system essential to operation of BES system and have low impact if compromised.
- A relay is essential to transmission line. How does it fit into overall BES reliability- low.
- Cyber asset essential to operation? Probe collecting info on penetrating.
- High voltage transformer is essential - high impact asset electrically. This protects from overloads, high impacts.
- Epiphany - cyber asset - RTU. In the substation. High impact to the substation. Where is the substation? Or generating plan. In high congestion part of system - loss causes other issues. In rural outpost different impact. Both cases it is a high cyber system.
- Has a high BES impact - rate asset as a 5. Can't view cyber asset in a vacuum by itself. Pay attention to BES ranking as well.
- Still conflicted order in which you do things.
- Confused - "essential cyber system." When talking about cyber impact - how could it be anything other than a high? Essential cyber system - digital relay not connected to anything. Cyber impact is low or medium. Same relay but talking to other relays, maybe a high cyber impact.
- Are we mixing threat, vulnerability and impact? That may be the source of the confusion.
- Cyber system could be everything or small - flexibility of deciding for yourself. Give a broadly scoped cyber system and narrowly scoped cyber system for the targets.
- CEMS e.g. of "targets"-- power plant only, substation only, control system only,
- 2 impact ratings. Analogy to FIPS 199.
- Categorized BES subsystems as drawn as 2 independent processes.
- If the arrow goes up to cyber systems and feeds into categorization.
- Change the terminology - want to end up with a categorized assets.
- Short cut - line distance protection relay. H/M/L to line protected. Apply that to all BES lines.
- Some confusion in the terms e.g. essential cyber systems vs. "critical".
- This is the impact part of a risk analysis. Don't focus on final result of numbers as they apply to protection. Going from categorization concept into protection concept. Should be based on threat and vulnerabilities.

- May be jumping here from impact levels- to target of protection without consideration of other elements - e.g. risk analysis, threat analysis? The leap from categorization to protection without reviewing the role of risk
- Missing piece - across the top - what is the impact of the cyber asset? Where it is? What substation in. What is the BES impact.
- May need a "susceptibility score"- how much control does it have, how is it connected? Is it a stand alone, dial up? What kind of operating system does it have? Consider these attributes to determine what is its impact?
- We will deal with some of this in the control side of the analysis. Mentioned in paper that we will deal with this in the assessment of controls.
- May need to deal with this in the working paper.
- More confused. Asset impact and cyber impact - if either is high, then it is considered high?
- Talking about tentacles of control system in assets - if I can get back into control system.
- Logistic management systems - broke into system - bar code readers -
- Think in terms of security in the event of an attack. Risk - high and low. On a given day, risk changes. Make sure you have it partitioned and cover.
- Are we over complicating this process? Overwhelming number in the industry are the smaller entities without the assets to perform this function. New piece - impact of identified cyber asset on the BES. What is the risk or probability? Big companies have resources to do this kind of work. Smaller ones don't have the capacity.
- Let's not use "risk" = financial exposure. Threat vulnerability of impact or possibly "susceptibility."
- Scott Fixmer offered the following process for evaluating facilities:
    1. Id facility assets and loss impact/consequence. By type of facility.
    2. If lose asset what is the criticality (10 different considerations)
    3. Characterize the threat- e.g. is a physical or cyber attack- what are the methods.
    4. Motivation and capability of those who might carry these out.
    5. Relative ease/probability of getting caught/ and of different types of attacks being applied to assets.
    6. Identify who the attacker is likely to be.
- This helps to sort it out but there may be more mitigating factors to apply. This may be most helpful when being audited- numerical ranking of criticality. Semi qualitative.

3. External Cyber Systems

Working Paper Section	*Avg.*	4	3	2	1	*Total*
External Cyber Systems	**2.6**	**2**	**7**	**8**	**0**	**17**

Member Comments

- How many who rated this low was due to the lack of detail? 2 ratings
- Reservations - hadn't gotten a clear representation - is this all inclusive? Service level or other contractual agreement - concern about the turf to cover. Not reliability based.
- This was like an external review topic.
- This may not be helpful.
- Remove or improve?
- Take it off line- there is a lot of work n terms of what this would be. This may be a distraction and may be technically infeasible.
- Many areas this could touch. Require lots of brainstorming to understand the scope of this.
- What do we expect from industry in reacting to this? Feedback on ideas or suggestions for improving
- In the NIST management world- impact analysis and categorizing, selecting controls is next. This is a consideration in selecting controls.
- If this is about the categorization, shouldn't mix with external.
- Is this a necessary segue way? Could it be pulled out?
- Interconnections section. Compress it and move?
- Middle bullet. Consider dropping the sentence?
- Thought of this in terms of EMS consultants.
- Put in something about need to coordinate?
- Vendor connection- vs. interconnection issues?
- You are relying on their data- integrity of that system. Some coordination with provider of data.
- This is exactly what we will see/hear from the industry. We are getting a preview in this discussion.
- This is a lot of work for a couple of people. Get more participation in these kinds of efforts.
- Analogous to 3rd party?

4. Categorization - BES Subsystems, Cyber Systems and Final Cyber System

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Categorization of BES Sub-Systems	**2.8**	**1**	**11**	**5**	**0**	**17**

Member Comments –Categorization of BES Sub-Systems

- More fine tuning need. This was intended as an overview
- Bright line concern with BES subsystem definition
- 3-categorization has to match the population of all possibilities - write definitions to cover the entire population. (45% of population covered?).

- Provide a quick list vs. the definitions provided. Top level or quick overview.
- This simply says categorized assets are needed - method and criteria will come later. Using VRF model of high/medium/low.
- Stop fixating on e.g. rank the criticality of BES assets somehow.
- Throws out as e.g. - industry has current CIP 002 and paper on risk assessment. Provide another example?
- Get together with the BES guys and tighten it up. Get RCs together (Jim Case, Jason, Jack Bernhardsen, etc.).
- References "event classifications" on NERC site - 5 categories. This might be a helpful analogous effort to describe levels. Specific when you see it you know which category you are in. Something along those lines? Look at this conceptually as a graded approach.
- When this goes out - lawyers and engineers will pick apart. Clarity and distinctiveness of the definitions. Will this be subject to too much speculation in terms of interpretation?
- Is industry capable of this? Many won't be able to do the analysis.
- NERC websites - events analysis - alerts, classification scale on left.
- Generator 800 mw, congested area - impact because environment around it compared with one in low congestion area. Approach - 2 identical plants in different parts of country don't have same impact.
- From a RC perspective, concern is stability. Clarify wording vs. examples. Pick something concrete.
- How does a cyber event correlate to these categories? Having a hard time in making the logical connections.
- Does nailing this down help us get our point across?
- Impact of making an impact decision. Scott Mix – items - who are we trying to cover with these standards. Internal problem before - CIP 002 self-selected out of process. Careful not to allow continue that behavior. Will this provide a loophole?

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Categorization of Cyber Assets	**2.8**	**2**	**9**	**6**	**0**	**17**

Member Comments

- Needs more detail and fleshing out.
- This highlights the complexity of the issue.
- Concern we could have cyber systems not associated with BES component with h/m/l. Components not part?
- EMS/ market management system ISO/ITO, not tied to BES components - huge amount of calculations across all different components - info for situational awareness.
- Goes back to cyber system that supports a BES function- good example of cyber system that directly support a BES function vs. a BES asset.
- Okay with words, they are not overly complex. Having to do stuff with BES first. Categorize cyber systems and protect. Leverage what is out there and use that.

- Original proposal- find cyber assets--establish high water mark- high will be high and may work in simplifying. Control center is a BES asset.
- Does the language in definitions, supported by examples, make it clear as to what they are and how to categorize them?
- Correlation between asset and cyber system. Functional piece is the good part. Agree on simplification. List of functions or impacts and then go find cyber systems and map to them. Must be the correlation because we don't know which are important. Hurdle of BES asset correlation part having trouble with.
- 800 mw in Connecticut vs. Texas. Cyber protection purely- does it matter? That today one has greater impact than the other. Does the BES asset impact mean anything?
- If you are a hacker - go at lesser impact asset and go from there.

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Final Categorization of Cyber System based on Impact to BES	**2.5**	**4**	**8**	**4**	**1**	**17**

Member Comments

- From cyber perspective- go for unimportant. Have to have some basic level of cyber security protection. Then may need additional protection. What that it is open to debate.
- Concerns in paper- ALR- credible contingencies don't relate to cyber issues. Don't inadvertently leave open.
- Target to get to h/m/l of systems. Leads to protected measures/controls. 003-009. Idea is to have a baseline set of minimum controls. Whatever low.
- Double impact language- asset correlation. Cyber categorization vs. impact.
- Agree we need to map the functions- through the lens of the assets or some other lens. Clarify that and the industry will understand.
- Numbers in box don't relate to audits?
- Applying controls in different ways? We will have set of controls apply to some and not to others. Threat landscape comes in. Once you get the target. Applying the catalogue- looking at moderate asset and apply controls in high way and that is what would be audited.
- If low BES impact?
- Controls are objectives- e.g. to put encryption in place. (Federal FIPS compliance).
- Five levels too complex. Three is sufficient.
- Government high/medium/low- federal sector it is applied to systems. TVA is a bad example.
- Double impact- how determine resulting impact. If you high water mark this, is this 1 size fits all/ all or nothing.

5. Identification of Essential Cyber Systems

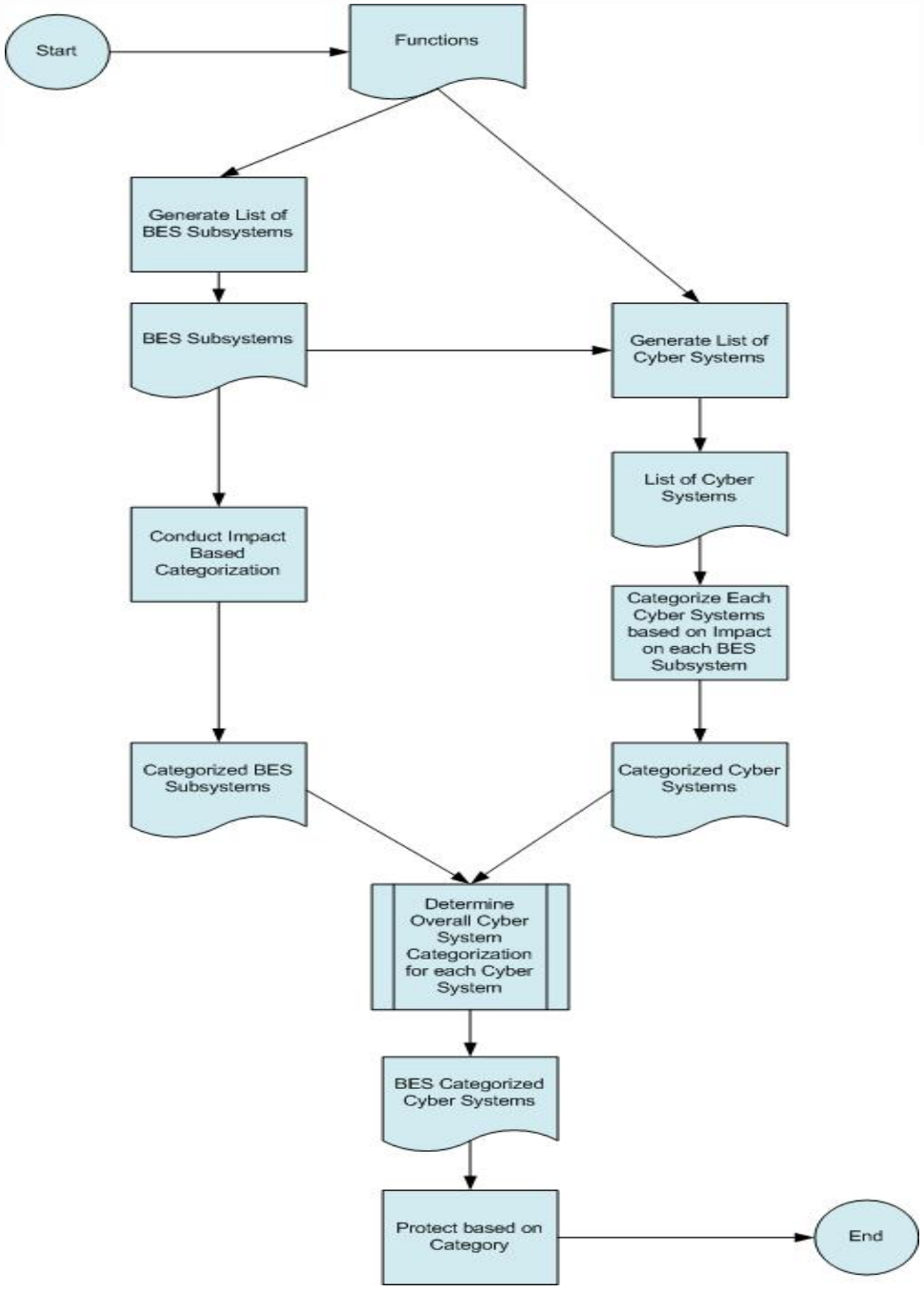
Working Paper Section	*Avg.*	4	3	2	1	*Total*
Identification of Essential Cyber Systems	**2.7**	**2**	**8**	**7**	**0**	**17**

Member Comments

- Was this meant to cover the entire population or an example? More work if intended to cover.
- Show why this would be critical. E.g. metering.
- "Essential"? Low impact essential- distinction- back office- real time. BES related cyber?

E. Review and Refinement of Working Paper Categorization Approach

On the second day, the SDT discussed whether to break into small groups to develop further guidance for refining the working paper. They considered breaking into groups focusing on: Categorization- BES, Cyber and Final; Identification of Essential Cyber Systems; and Target of Protection & External Cyber (including working on chart). They decided to have an open discussion of the categorization concept followed by the development of at least one or more scenarios to put it to a test.



1. Open Discussion on the Categorization Approach

Member Comments

- How should we approach categorization- from cyber systems or from BES asset/sub systems and then looking at cyber systems? The matrix has brought the discussion out.
- At this juncture- may need to take a second step in the matrix.

- Do we need the matrix anymore? Maybe we should talk about different concrete examples in order to identify the benefits and drawbacks of two approaches to categorization. Take an example of a cyber system approach and an example from a BES asset perspective and see if we would come up with the same cyber system.
- Reclamation's experience with 16 SCADA systems. In mapping those to the mission, people came up with different answers and not just a single interpretation for different systems and projects. In the Federal process, everything is included by default- CIP doesn't get this. FIPS 199 divides them up.
- Test cases- can make the correlation between the asset piece and the cyber asset.
- Smaller entities easier to get the cyber part?
- Don't forget that the "C" in CIP is critical not cyber. Critical BES assets that don't have a cyber component.
- We may need a SAR for physical security standards.
- NERC recent response to DHS – clear classification tier 1-3 assets- high med low- megawatts.
- Test both approaches- if both get you there. Pick the simpler one to go to the industry with.
- There is agreement on the approach. We have just engineered something and we need to test it. Will it produce the result we are looking for? The industry will also test this.
- Do we have enough details to test the model?
- FIPS 199- hard process- to get categorization process. Federal starting with a system. Tied to business/mission and mapped the two together.
- Biggest concern that is driving the parallel approach is making sure the impact of BES asset is considered when protecting cyber asset.
- Can we account for the impact of the BES asset without going through the left side using a pure cyber approach? That is the piece to test for the cyber approach.
- If both approaches work, we then agree on a couple assumptions.
- Does the actual impact of BES asset, based on where you are in the grid, have any bearing on how you protect the cyber asset?
- Lots of time, money and vested interest involved in this. In the end, we have to produce a set of standards that can be implemented by the industry, consistently complied with by the industry, from Pinecone Power to the large utilities.
- SDT has been struggling with this in terms of the overall complexity.
- You do protect your cyber assets differently. I pick PLC system in a sub station identical to one in another substation. I shouldn't need to protect at the same level. We will have more controls on the more essential system. Don't see it as overly complicated. I don't think you can come to that result by just working down the cyber side.
- "Back in the day"- cyber linkage to engineering. Don't have to sell the need any more. Cyber important. Access can be gained to trivial equipment. General frame of reference. We don't have to sell the need for linkage quite so hard.

- DHS Tiers 1, 2, 3. It is similar to the left side. If it makes sense and it helps us, it serves our purposes.
- Going to have to both- electrical assets focus- where I roll out protection. Not a one vs. the other?
- Possible test candidates considered: balancing Authorities- Test AGC from the cyber side. Test a transformer over current. Pick a restoration. Control and Operation and Load Balancing- 2 functions? Calculate ACE? Load Management-Function- Control and Operation. 2 transmission and generation operations.

The SDT broke before lunch and a small group developed the following scenario that was presented and discussed following lunch:

Scenario: A large investor-owned utility with 35,000 MW generation capacity across 103 units. One of their plants has three 800 MW generating units. A single RTU receives the control signals (pulses or set-points) for all three units. Each unit is managed with its own PLC/control system. From a span of control perspective, the SCADA/EMS at the generation control center can potentially control or impact all 35,000 MW of generation capacity.

Discussion: It does not matter whether the units are base loaded, on regulation, in reserve, or running at their maximum capacity. It is what the control system is capable of impacting, not what it can impact at this moment in time. If the SCADA/EMS can open plant substation breakers and disconnect the units from the grid, the system impacts that generation whether or not the SCADA/EMS is actually directing generation output (sending the units raise/lower pulses or MW set-points). The RTU in the plant is managing the telemetry data for all three 800 MW units, thus it can impact 2400 MW of generation capacity if it is compromised. The PLC/control system for each unit only controls its own unit, thus its impact is 800 MW. In the scenario, the SCADA/EMS system would have been categorized as High Impact, the RTU as Medium Impact, and the PLC/control system as Low Impact.

Presentation of the Scenario

- Factored in the impact of BES asset in identifying cyber assets performing the function. Identify cyber assets- may be supporting BES asset and have a greater impact.
- 2nd control system used for monitoring /situational awareness- could be pressed into service to control under abnormal situations. It has a capacity to control- not what it is used for. Ergo- higher impact based on what it potentially can do, not what it normally does.
- ICCP node - low- it can go away, I don't care. System not that important to our operations but it may be to some one else.
- All 3500 mw to reliability coordinator via ICCP. From RC perspective it is high.

- I am sending 3500 mw info to RC- categorize as a high- because of what it is actually and what is it capable of doing.

Member Comments on the Scenario and the Categorization Approach

- "Span of control" notion is critical
- If you did it from BES side get to the same result.
- It was essential to setting up scenario- to start with BES functions. It is the branching underneath we are struggling with.
- System Frequency for AGC considered? Yes. How do you ensure you haven't missed something from an audit perspective?
- How to demonstrate to auditor under CIP 002- that you are at least mapping the functions.
- When you de-construct the functions and look at interactions necessary to support the function.
- The key is you started with function.
- Standard should seek to ensure effectiveness. Are you protecting the right thing and how well protecting is the next phase? Could overlook a core piece – in 002 specify mandatory criteria you have to look at.
- If I didn't look at substation first, I wouldn't have known of the problem upstream.
- Factors in BES asset impact with span of control without having to categorize the BES asset.
- Class the RTU as a medium. 2400 mw plant depending on where it is could be low or high in terms of BES impact. Because of where it is and its impact on BES.
- System impact assessment based on modeling of BES - lots of work. NPCC has done it that way.
- Start with impact of asset on the BES.
- Should we give the entity the choice to which side to chose?
- BES asset view point - system conditions change.
- Problem on the Cyber side. Restoration- how to identify a cyber system that supports restoration for a cranking path? Starting from cyber side - numerous elements in BES system- to identify what cyber systems are related to them. A cyber system can support multiple BES functions. Find all cyber assets in the cranking path. Will first find the BES assets.
- Do you need to categorize and impact assess? Yes you do.
- Don't mix cyber and physical systems?
- Some functions it may be done, other functions it may not be done.
- Missed common load generator.
- Sounds like we are saying we need to do both. Eliminate arrow between the 2 paths.
- Cyber perspective - span of control concept on BES side - merge together have a super list. Not two competing process. In the end consider BES. If only do left side you may miss or lower the rating mistakenly.
- Focus on cyber subsystems that directly support BES.

- It is iterative approach (but back and forth, not circles).
- Two parallel supporting efforts to get a super list vs. one subordinate of the other.
- Goal of a categorization of cyber system- consistent methodology.
- Implicit in doing both approaches is the assumption that you have an incomplete inventory on one side or the other. If you had a complete inventory of cyber assets do that side only. With a complete inventory of BES, do that one side?
- Give some more flexibility to do what they want
- Horizontal line should go away at top. Impact assessment of BES assets is a question of what to address first. The impact of BES asset shouldn't alter the level of the
- Generate list of BES subsystems under functions. One system supports moving power and one that support analysis and wide area view.
- It is the "span of control" that we are driving at.
- We are not asking the entity to devise a methodology to do an impact categorization. Standard will provide the criteria to assess and categorize their assets.
- Planning uses catastrophic conditions as a base.
- Try to remove the impression that one side is subordinate to the other. However can't be done in a vacuum. Have to understand the electric system.
- Try to create a single line for the diagram?
- If IT, supporting operations side of business. Start with generating list of cyber systems. Will have a hard time completing an assessment. If you don't start with functions - how do you know?
- The standard needs to give industry the criteria for the categorization.
- Give a list of functions? Will that change -
- Operating functions - these have already been defined by the industry. Version 5 of the functional model -
- However, note that functions are different from functional model. E.g. Entergy - single registered entity with six different functional models. Implementation convention within the organization.

- The reliability functions are applicable to you. Functional model - is not that clean.
- Rely on the functions and then map to BES and cyber assets. Will need lots more detail in the boxes in terms of text explaining the boxes.
- If you took BES analysis - called it "criticality" of specific elements - Cyber analysis- look at consequence of compromising and give it ranking. Where is the synthesis point - gives your impact. Take impact merge with "susceptibility" - and get to your impact
- Interconnectivity is at play? Yes.
- Do we want to say in certain areas of the working paper that the SDT is not sure of the answer? We need to present something with conviction, but not at a great level of detail.
- Link the last box to the next process
- Like the model that has emerged, it should be consistent with the Working Paper but not as detailed. Reflects more flexibility and identifies the big concepts.
- Bottom box is the outcome of the process- identifying what you need to protect- and arriving at the appropriate categorization
- What is the span of control?

- Existing 002 and this? Wrapping all within the reliability function. Every BES asset will be protected at some level.
- Can the SDT live with this conceptual graphic depiction for inclusion in the working paper? Yes.
- Can I go through this? Can't disregard but may not start with inventory of BES assets.
- What is the expectation of the BES analysis, i.e. what will be done with the analysis? All cyber assets inventoried.
- What to do with the BES analysis. Not all 115 relays need the same protection.
- BES analysis? What if left fed into the right vs. working in parallel. Feed this into cyber analysis/ span of control exercise?
- Default BES analysis is high - then purely assessment of cyber assets.
- BES changing all the time? System accounts for contingencies. Changing so much? No.
- We need 75-80% of relays to work when we need them.
- Consider US DHS - Tier I II Critical assets each sector tasked to come up with criteria based list. How to figure out where "big uglies" are. Tier 1 - most impactful. High capacity, high voltage. Tier 2 - size and scope. Tier 3 - everything else. This could eliminate the need for extensive analysis.
- Conceptual language drafted to codify into a standard. This becomes the analysis-identify and classify as a mapping exercise - Find cyber assets BES mapping (criteria) and analysis (use DHS tiers)
- Is this an external process? BES system comparing against criteria?
- Does BES mapping belong here? External process to this sequence? Entity still must categorize. Something needed to verify that mapping is still correct?
- Do once a year. Don't devise the criteria every year. Established outside an entity's process.
- Criteria should appear in a Reliability Standard.
- BES Subsystems vs. assets. Control center are included.
- Restoration is included in Tiers 1,2, + 3.
- Does this pull distribution into criteria?
- IT is a linear model with the same components. Using the DHS = tiers as a departure point. Stand alone standard.
- Perhaps CIP 002 (include the tiers) and CIP 003 features cyber characterization

Member Final Comments on the New Graphic

- Broad support for this depiction on SDT.
- Both start with reliability functions. This is a single vs. parallel path.
- This has BES mapping.
- Big difference - don't need 3rd party oversight of categorization of subsystems.
- More a performance based model - how well did you do the mapping and applying the controls.
- Less a black and white compliance exercise.

- How big a deviation with the current document? Language may need to be clearer that criteria will be provided.
- The diagram doesn't conflict with philosophy behind the working paper.
- Scope of impact and span of control are good concepts.
- SDT should plagiarize content of DHS- refer in more general terms. If want to avoid confusion, pick up concepts without numbers.

2. Identification of Essential Cyber Systems

Member Comments

- Other synonyms for "Essential": Vital, crucial, fundamental, critical, Quintessence-Imperative, indispensible, germane, etc.
- BES cyber systems. Intent to distinguish market systems. Corp cyber assets - we don't want to think about. Control systems and things impacting control systems.
- Is more information needed on "essentiality" criteria mapping? Cross sector cyber security working group.
- Sam Merrill's document? Scott will get this and share it with SDT.
- Equivalent levels between bulk and cyber side. E.g. non routable no longer an in/out criteria. Everything is in, but to a degree.
- Ramifications for Canadian? If DHS, tier 1 and tier 2. If the Canadians can adapt or augment, based on these concepts, there is no issue, much like NIST.

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

1. Drafting Group Follow Up Steps before Vancouver

Members expressed thanks and appreciation to all those participating on the Drafting Team and to John, Phil and Jackie for leading a tremendous effort in "taking us down this road." John Lim agreed to work with Phil Huff and all other interested SDT members to:

- Produce the next draft which will be circulated as a final draft for consideration and adoption in Vancouver before seeking industry comments on the concepts.
- Take the SDT comments on the "target" section and produce another graphic using an alternative depiction.

The following members agreed to joint the drafting group: Dave Norton, Dave Revell, Jon Stanford, Joe Doetzl, Jay Cribb, Jim Breton and Kevin Perry. The BES experts will be joining and working with the team as well. NERC produced a 2 page statement of work for the experts: they will help finish working paper and requirement statements; be available to respond to draft posting comments associated with pieces; and have no expectation of a need to travel.

There will be additional working papers developed for SDT review going forward including:

- BES Risk Management concept paper
- Security Control concept paper.

IV. NEXT STEPS

A. 2009 SDT Workplan Approach and Schedule

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 rounds of comments from the industry before going to the ballot.

Member Comments

- Regardless of what the controls are, nothing/no one will be able to tell us how to solve the CIP 002 challenge. This is clear in reviewing the five competing bills in congress.
- The SDT should stay as focused on CIP 002 related. Let the political winds blow wherever.
- Always will think about controls and some hierarchy. We should focus on the "what" in the short term.
- For the SDT December release- we should consider picking some security control to give as an example as to what it means in terms of high medium low on a password protection.
- We don't have too bad a set of controls- 003 -009 will serve us for a little while.
- Focus on CIP 002 only? A little bit of both.
- Flagging issues for the industry that need to be done.
- Highly desirable –the sooner we get the concept out to industry the more time they will have to read and digest.
- Decoupled approach, multiple levels of analysis- more time they have to get comfortable with concept, the better.
- Industry will provide us with comments.
- When the operating people got on the team. Reaction was surprising- they pointed out that this is really a paradigm shift from the operating standpoint.

The Chair reminded people that the SDT would try to establish the 2010 meeting schedule at the July SDT meeting in Vancouver, B.C. Canada. For the time being she noted that the August meeting will take place as scheduled in Chicago pending confirmation of available meeting space. SDT will be notified soon if we need to change locations.

B. Other Items

Dave Norton advised the group of a call for self-nominations closing on June 25 for a new SAR drafting team which would be defining next generation of situational awareness control tools for the BES. Going out to operations and planning only. This is fundamentally a systems

project - command and control, remote telemetry. Part of what they want to do is constrained by what actually can be done. He suggested this will be highly interrelated with the 706 SDT's efforts and they will need more cyber perspectives from people who know how to run high speed wide area networks. It will be related to the further development of the smart grid and the use of the internet. He believes presently there are mostly vendors and academics interested in serving as members. As all of these intersect at the BES there is a need to get involved, and provide some cyber visibility.

He also noted that a big document was released today on 291 smart grid interoperability.
http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf
It has a big section on cyber security with lots of financial resources behind this effort. The report's introduction includes the following context:

> "In early 2009, responding to President Obama's energy-related national priorities, NIST acted to accelerate progress and promote stakeholder consensus on Smart Grid interoperability standards. On April 13, NIST announced a three-phase plan to expedite development of key standards.
> This document is input into the first phase: engaging utilities, equipment suppliers, consumers, standards developers and other stakeholders in a participatory public process to identify applicable Smart Grid interoperability standards, gaps in currently available standards and priorities for new standardization activities.
> NIST awarded the Electric Power Research Institute (EPRI) a contract to engage Smart Grid stakeholders and develop a draft interim standards roadmap; NIST will use this document as a starting point in developing a NIST interim "roadmap" for Smart Grid interoperability standards. EPRI technical experts compiled and distilled stakeholder inputs, including technical contributions made at two EPRI-facilitated, two-day, public workshops. Other inputs include the accomplishments of six domain expert working groups established by NIST in 2008, and the cyber security coordination task group established in 2009. To date, hundreds of people have participated in the road mapping process."

C. Closing

The Chair thanked Jon Stanford for hosting the meeting and noted that she and Kevin appreciated the spirited debate that was honest, painful, but did make some progress in particular refining and simplifying the flow chart. The SDT is now aware of the concept of paradigm shift and will continue to incorporate broad spectrum of background and experiences represented around the table. Once again she thanked the Drafting Group members for an outstanding job.
Members completed an onsite meeting evaluation form *(See, Appendix #3).*
The SDT adjourned at 3:00 p.m. on June 18.

Appendix # 1
Project 2008-06 Cyber Security Order 706 SDT
Draft Meeting Agenda
June 17, 2009 | 8:00 a.m. to 5:00 p.m. PDT
June 18, 2009 | 8:00 a.m. to 5:00 p.m. PDT
Bonneville Power Administration
905 NE 11th Ave
Portland, OR

Proposed Meeting Objectives/Outcomes

- Receive update on TFE and VSL/VRF processes
- Receive update on the SDT "Key Messages Task Group"
- Review and refine the CIP Version 3 Working Paper as a conceptual framework going forward in plenary and small groups;
- Agree on next steps in the Work plan and assignments.

Draft Agenda
Wednesday June 17, 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 May 13-14 Boulder City meeting summary and adoption

8:20 a.m. Review of Meeting Objectives, Agenda and Meeting Guidelines - Jeri Domingo Brewer and Bob Jones

8:30 a.m. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure - Scott Mix
Update on VSLs/VRFs - Scott Mix

9:20 a.m. Overview of Steps to Date in the SDT CIP Version 3 (Phase 2) Development Process - Stu Langton

9:40 a.m. CIP Version 3 Categorizing Cyber Systems Working Paper - Big Picture Concepts Presentation - John Lim, Jackie Collett

10:45 a.m. Break

11:00 a.m. CIP Version 3 Working Paper Review and Discussion of Key Outstanding Issues - John Lim, Jackie Collett, et al

12:30 p.m. Working Lunch (Return to plenary meeting at 1:15)

1:15 p.m. CIP Version 3 Working Paper Review and Discussion of Key Outstanding Issues - John Lim, Jackie Collett, et al

	Test for SDT Consensus and Endorsement of Big Picture Concepts
2:45 p.m.	Consider Small Group Key Issue Breakouts
3:00 p.m.	Break
3:00 p.m.	Small Group Discussion of Key Outstanding Issues
5:00 p.m.	Recess

Thursday June 18, 2009

8:00 a.m.	Welcome and Agenda Review
8:10 a.m.	CIP Version 3 Small Group Reports – Plenary Session
10:00 a.m.	Break
10:15 a.m.	CIP Version 3 Small Group Reports – Plenary Session
12:00 p.m.	Working Lunch
12:45 p.m.	CIP Version 3 Working Paper(s) Refinements and Discussion - Small Group or Plenary
2:45 p.m.	Break
3:00 p.m.	Next Steps and SDT CIP Version 3 Process Working Paper(s) Assignments Initial discussion of CIP 002 Version 3 SDT Subgroup Structure in 2009 (Requirements, Measures, etc.) Consensus Testing of Development of CIP 002 Version 3 for Industry Comment and Ballot in early 2010 apart from Other CIP Standards Review of Next Steps and Work Plan
4:30 p.m.	Review July Meeting Objectives
4:45 p.m.	Meeting Evaluation - Review June Meeting Progress (What was accomplished? What helped? What can be improved going forward?)
5:00 p.m.	Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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. Jeri Domingo-Brewer, Chair	**U.S. Bureau of Reclamation**
3. Jay S. Cribb	Information Security Analyst, Southern Company Services, Inc.
4. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
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
Richard Kinas	Orlando Utilities Commission
10. David Norton	Policy Consultant, CIP Entergy Corporation
11. **Kevin B. Perry, Vice Ch.**	Director, Critical Infrastructure Protection, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Jonathan Stanford	Bonneville Power Administration
16.Keith Stouffer	National Institute of Standards & Technology
1. Roger Lampilla	*NERC*
2. Scott R. Mix	*NERC*
3. Joe Bucciero	*NERC/Bucciero Assoc.*
4. Robert Jones	*FSU/FCRC Consensus Center (Wed. & Thursday)*
5. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via Webex/Phone

17. Jim Breton	ERCOT
18. Jackie Collett	Manitoba Hydro
19. Scott Rosenberger	Luminant Energy

SDT Members Unable to Attend

1. Sharon Edwards	Duke Energy
2. John D. Varnell	Technology Director, Tenaska Power Services Co.
3.William Winters	Arizona Public Service, Inc.

Others Attending in Person

Darrell Hobbs	NU Energy
Chris Ewing	SEL
Curt Wilkins	BPA
Kim Long	Duke Energy
Forrest Gist	CH2MHill
Clark Goodlett	CH2MHill
Robert L. Windus	CH2MHill

Others Attending via Webex/Phone

James Bassett	Lafayette
Steve Dougherty	
Mike Fischette	
Travis Jaffrey	
Jason Marshall	Midwest ISO
Sam Merrell	CERT
Hoang No	
Mike Peters	FERC
Chris Wright	Burns & Mac

Appendix # 3 Meeting Evaluation Feedback

CYBER SECURITY ORDER 706 SDT
JUNE 17-18, 2009, PORTLAND, OR
MEETING EVALUATION FEEDBACK FOR INCLUSION IN FACILITATOR'S REPORT

Use the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree. A summary of the SDT responses will be placed in the Meeting Summary

1. Please assess the overall meeting.

7.5 The agenda packet was very useful.
8.0 The pre-meeting paper (Working Paper) was very useful.
8.5 The WebEx document display and the audio were effective
9.4 The quality of the meeting facility was good.
9.0 The objectives for the meeting were stated at the outset.
7.4 Overall, the objectives of the meeting were fully achieved.
Were each of the following meeting objectives fully achieved:
9.3 Receive update on TFE and VSL/VFR processes
N/A Receive update on the SDT "Key Messages Task Group"
7.4 Review, refine and adopt the CIP Version 3 Working Paper as a conceptual framework going forward in
plenary and small groups;
7.9 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.

8.3 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
8.8 The Facilitators made sure the concerns of all members were heard.
8.5 The Facilitators helped clarify and summarize issues.
8.0 The Facilitators helped members build consensus.
8.6 The Facilitators made sure the concerns of all participants were heard.
7.3 The Facilitators helped us arrange our time well.

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

7.8 Overall, I am very satisfied with the results of the meeting.
8.3 Overall, the design of the meeting agenda was effective.
8.7 I was very satisfied with the services provided by the Facilitators.
8.0 I am satisfied with the outcome of the meeting.
7.3 I am satisfied with the progress we are making as a Team.
8.8 I know what the next steps following this meeting will be.
8.4 I know who is responsible for the next steps.

4. Other comments (use other side)

It's just painfully slow…So was building Rome…☺

What did we achieve?

- Significant breakthrough on working paper concept
- Synthesis of the BEX/Cyber process tracks
- We got the entire team on-board with the document. Progress was made, but was painful
- Refine flow-chart

What are our biggest challenges going forward?

- Team acceptance of revisions stemming from meeting
- Industry acceptance of new approach
- Getting something done before congress tells us what to do!
- Finalizing the concept paper
- Organizing the SDT to evolve the standards

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

- Try to control chasing of rabbit trails
- Put end to repetitive arguments/discussions
- Don't know what…
- There should be a more cncerted effort to research existing work (such as the DHS Tier I/Tier II document) that may be beneficial to the progress of the group
- Organize for results
- Smaller groups
- Iterative development
- Organize by capabilities
  - Experience
  - Capability/expertise
  - BES function
  - Interest
- Too much open group dialogue – letting 25 people weigh-in on all issues is
- arduous/counter-productive.
- We need to come to each meeting ready to make decisions – Decide/Act

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

CYBER SECURITY ORDER 706 SDT MEETING SCHEDULE

OCTOBER 2008-DECEMBER, 2010

DEVELOPMENT OF CIP FRAMEWORK OCTOBER 2008-JULY, 2009

1. October 6-7, 2008, NIST, Gaithersburg, MD, Review of CIP 002-009, Agreement on Phase 1/Version 2 approach
2. October 20-21, Sacramento, CA, Phase 1/Version 2 Development
3. November 12-14, 2008, Little Rock, Phase 1/Version 2 Adoption; Phase 2/Version 3 Process review
4. December 4-5, 2008, Washington D.C., Phase 2/Version 3 review and debate, white papers assigned.
5. January 7-9 SDT Meeting, Phoenix, AZ ½ / 1/½ 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.

6. February 2-4 SDT Meeting, 2009, Phoenix, AZ, ½ / 1/½ day format. Mon-Wed.

- Update on NERC Technical Feasibility Exceptions process
- Review of VSL process and SDT role
- Review of Phase 2 White papers, strawman and principles
- Review and Adoption of SDT Responses to Industry Comments on Phase 1 and Phase 1 Product Revisions.

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

- Update on Phase 1 process
- Update on NERC TFE process
- Update on VSL Team process
- Review, discussion and refinement of Phase 2/CIP 002 White papers, strawman and principles

8. 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 2 CIP 002 Strawman 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 1 Ballot Results (*Quorum: 91.90% Approval: 84.06%) *and Industry Comments-*

9. April 14-16, SDT Meeting, Charlotte NC, ½ / 1/½ 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 1 Industry Comments- Recirculation Ballot
- Review and Refinement of Phase 2 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.

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

- Review MRC presentation and any input to SDT on Phase 2 approach
- Further SDT refinement and discussion of the Phase 2 White Paper.

June, Working Paper Drafting Team Meetings/WebEx, June 8 & June 15, 2008

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

- Further SDT refinement of the Draft CIP Version 3 Working Paper(s).
- Review SDT development process for June-December 2009
- Discuss potential SDT subcommittee structure and deliverables.

June, WebEx meeting(s)

- Working Paper Sessions including inputs from selected industry personnel to help establish BES Categorization Criteria
- Agree on and charge SDT subcommittees

12. July 13-14, 2009 Vancouver, B.C., Canada

- SDT Plenary session to review and respond to any input/comments on Working Paper
- Adopt Version 3 CIP Working Paper for industry review
- Confirm SDT Subcommittees and Deliverables
- Conduct subcommittee organizational meetings
- SDT Subcommittees meet to begin drafting assigned issues and deliverables
- Subcommittee organizational and deliverable reports to SDT

July, WebEx meeting(s)

- Working Paper Sessions including inputs from selected industry personnel to help finalize BES Categorization Criteria
- SDT Subcommittee meetings (as needed)

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

13. August 20-21, 2009, Chicago IL

- SDT Plenary session to review and respond to any industry input/comments on Working Paper
- SDT Plenary and Drafting Subgroup meetings to develop and test support for deliverable CIP 002 provisions

*August, 2009, **NERC Member Representative Committee***
Progress Report and presentation on new CIP Version 3 Working Paper-Concept-Reliability Standards on Cyber Security for MRC input, Winnipeg, Manitoba

August, WebEx meeting(s)

- SDT Subgroup meetings (as needed)

14. September 9-10, 2009 Folsom, CA

- SDT Plenary session to review and respond to any additional industry input/comments on Working Paper
- SDT Plenary session to review MRC input on approach to Version 3 CIP Reliability Standards on Cyber Security and consider and agree on refinements

- SDT Subgroup drafting meetings- prepare deliverables
- SDT Plenary Session(s)- provide briefings and Subgroup reports
- Review Work Plan through Summer, 2010, as needed
- Establish SDT Meeting Dates and Locations for Jan-December 2010

September, WebEx meeting

- SDT Subcommittee drafting meetings

15. October 20-22, New Orleans LA

- SDT Subgroup drafting meetings
- SDT Plenary Session(s) - Subgroup reports on CIP 002 deliverables
- SDT Subcommittee drafting meetings
- Review, Revise and Adopt Work Plan through Summer, 2010, as needed
- Confirm Meeting Dates and Locations for Jan-December 2010

October, WebEx meeting

- SDT Subcommittee drafting meetings

16. November 17-18, Atlanta GA

- SDT Plenary Session(s) – to review and refine CIP 002 deliverables from SDT Subcommittees
- SDT Subcommittee drafting meetings to refine products based on SDT input

November, WebEx meeting

- SDT Subcommittee drafting meetings to finalize drafts

17. December 15-17, Tampa

- SDT Plenary Session(s) to review, refine, and agree on and adopt CIP 002 deliverables of new Categorizing BES and Cyber Systems Standard
- Agree on initial Posting of draft CIP 002 for industry review and comment

December, WebEx meeting

- SDT Subgroup meetings

DEVELOPMENT OF OTHER CIP STANDARDS- JAN.-DEC 2010

SDT Meetings 18-30. 2010 *(12 SDT monthly meetings and subgroup webex meetings as needed)*

- SDT Responds to Industry Comments on Initial and Subsequent Postings of CIP 002, Version 3 *(may be multiple comment periods, as required)*
- Refine the CIP 002 and submit new CIP 002 Version 3 Standard for Balloting while permitting industry to rely on CIP 003-009 until the full suite is reviewed and presented for balloting.
- Initiate Development of the full suite of CIP Reliability Standards on Cyber Security including Requirements, Measures, Controls, etc.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP Standards for Industry Ballot
- NERC Board of Trustees Adoption of the full suite of Standards
- FERC Approves and NERC Implements the full suite of CIP Standards

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 6 Phase II Working Paper

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

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706
06/15/2009 –Team

This draft Categorizing Cyber Systems paper is a “Work in Progress” that is meant to convey the initial thoughts and ideas that should be addressed and considered by the full CSO706 SDT as part of the deliberations related to the revised CIP Reliability Standards addressing Cyber Security. This is a Working Concept Paper, and is subject to change as these initial concepts are addressed and discussed by the SDT.

TABLE OF CONTENTS