NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

July 13, 2009 | 8 a.m.–5 p.m. PST
July 14, 2009 | 8 a.m.–5 p.m. PST
Vancouver, British Columbia, Canada

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

Joe Bucciero, Bucciero Consulting, LLC

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

Adopted by SDT 706, August 21, 2009

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary Contents

Cover 1
Contents 2
Executive Summary 3

I. Introductions, Agenda Review and Review of SDT Workplan **5**
II. Updates **5**
A. Technical Feasibility Exception, NERC Rules of Procedure Posting 5
B. VSL/VSRs 7
C. Other Related Cyber Security Initiatives 7
III. CIP 006.1 Interpretation **8**
IV. SDT 706 Phase II/Version 3 Development Process- the Working Paper **9**
A. Overview of Phase II Workplan 9
B. Concept Paper Presentation, Review and Adoption 9
V. Development of Concept Paper Announcement and Comment Form **11**
VI. CIP-002 Subgroups **13**
A. Introduction, Appointment and Charge to CIP-002 SDT Subgroups 13
B. Subgroup Organizational Meetings and Comment Form Questions 14
1. Reliability Functions 14
2. List of BES Subsystems and/or BES Cyber Systems 15
3. BES Mapping 15
4. Cyber Analysis 17
5. Definition and Selection of Controls 17
C. Subgroup Guidelines 18
VII. Next Steps and Closing **18**
Appendices Table of Contents 19
Appendix 1: Meeting Agenda 20
Appendix 2: Meeting Attendees List 22
Appendix 3: Meeting Evaluation Summary 24
Appendix 4: NERC Antitrust Guidelines 26
Appendix 5: SDT Work plan Schedule 28
Appendix 6: CIP-002 Work plan Proposal 31
Appendix 7: CIP-002 Subgroup Assignments 33
Appendix 8: SDT Version 3 Points of Consensus- April, 2009 34
Appendix 9: Working Paper: Categorizing Cyber Assets: An Approach Based on BES Reliability Functions 35
Appendix 10: Herding Cats 101Tips for Small Group Discussion and Shared Leadership 37
Appendix 11: Draft Announcement-Concept Paper 39

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer and Vice Chair Kevin Perry welcomed the members. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the team and participants the proposed meeting agenda.

Mr. Bucciero reviewed 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 cover all participants and observers.

Kevin Perry made the presentation the Technical Feasibility Exception (TFE) and the NERC Rules of Procedure posting and Gerry Adamski, NERC's Director of Standards offered additional information on behalf of Scott Mix who was not able to attend the meeting. Kevin noted several areas that are under review and Mike Assante was leading a "tiger team" with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Gerry Adamski noted the plan to submit to NERC Board of Trustees for review and adoption at the upcoming August meeting has been delayed until the next BOT meeting in the Fall given the open issues and the need to clarify the implications and questions for NERC's implementation including how to capture the process in the 2010 plan and budget. NERC hopes to produce a final TFE process sometime next year before FERC. The members discussed the range of questions and issues that had been raised by the industry and both the interim and final TFE.

David Taylor provided an update report to the SDT on VSLs and VRFs noting that he does not expect that the SDT will need to address or deal with this going forward as the assigned SDT is handling the process. The SDT discussed the Smart Grid effort that is being led by NIST. Keith Stouffer reported that the effort is addressing system level requirements from the top down and component level details from the bottom up. They are working with 800-53 NIST and ISA 99 work and are keenly aware of the work of the SDT. He also referenced the work now on ISA 99 — Part 4 — detailed cyber security for industrial control systems. These requirements will be harmonized with other activities.

NERC requested that the SDT review its CIP-006-1 Interpretation. The CIP Standards Interpretation Team met the first day over lunch to reconsider the interpretation of CIP-006-1 requested by SCE&G regarding the need to physically protect Critical Cyber Assets that are dial-up accessible but do not use a routable protocol. The interpretation was previously approved by the industry but not yet submitted to the FERC for approval. The interpretation asserted that the exclusion of such Critical Cyber Assets is a correct interpretation of the standard. The team examined CIP-002-1, CIP-005-1, and CIP-006-1, along with the FAQ for the Version 1 CIP standards and determined that the exclusion might not have been written had the standards been developed with present day knowledge, the interpretation team agreed and the SDT concurred that the interpretation approved by the ballot body and the NERC Board of Trustees is a correct interpretation of CIP-006-1, Requirement R1.1.

Stu Langton reviewed the milestones in Version 2 and Version 3 of the SDT work and the SDT convergence on a single consensus approach in Orlando that was refined further in Charlotte, Boulder City and Portland with John Lim and Phil Huff leading an expanded drafting team to continue to refine the paper between meetings. Joe Bucciero, with the SDT facilitation team, reported that following the Portland meeting the SDT has been supplemented with additional members and BES expertise and has produced its proposed concept paper for the SDT's review and adoption.

On behalf of the SDT, the Chair thanked John Lim, Phil Huff and the other members of the drafting team for working productively since the Portland SDT meeting and bringing to Vancouver a proposed concept paper that can be adopted by the SDT for sharing with the industry as the basis for the SDT's efforts in developing the Version 3 standards. John Lim presented the working paper noting the significant changes and improvements that emerged from the Portland SDT meeting. The SDT discussed the paper, agreed to some minor wording changes and agreed that the paper would be archived. The SDT agreed that industry comments should be focused on the development of CIP-002 requirements in the key areas set forth in the concept paper. Following the discussion the SDT unanimously adopted the concept paper as revised for sharing with the industry and agreed to develop a draft cover letter and comment form for posting with the paper. The team discussed a "game plan" for communications with the industry on the working concept paper and agreed to post the paper, brief the Members Representative Committee and present a Webinar in August and provide an update on progress at the NERC October workshop in Dallas, Texas.

The Chair reviewed the July-December 2009 work plan proposal circulated in advance noting that all members of the SDT would participate in at least one of five proposed subgroups drawn from the concept paper, (i.e. Reliability Functions; List of BES Subsystems and/or BES Cyber Systems; BES Mapping; Cyber Analysis; and Definition and Selection of Controls. Member noted their preferences and the Chair and Vice Chair made assignments guided by those preferences. Each subgroup was charged to draft requirements for consideration by the SDT to be included in a draft CIP-002 Version 3 to be shared with the industry in December 2009.

On the afternoon of the first day and the morning of the second day the five subgroups met in parallel conducting organizational sessions to: review scope of the assigned topic; identify areas that may need development of related CIP-002 requirements; determine what information they will need going forward; select a leader/spokesperson, a scribe and a timekeeper; sketch out a work plan, including a meeting schedule in order to get the work done by the October SDT meeting. Finally the subgroups were asked to draft questions for their topic for use in the concept paper comment form.

The SDT discussed the roles that would be played by the members, subgroup members, subgroup leaders, and a coordinating team and staff. On the second day the SDT agreed that it would be helpful to develop a set of consistent coordination guidelines for the subgroups.

The Chair reviewed the schedule for getting the concept paper, announcement and comment form finalized and posted on the NERC website for industry comment. She expressed the hope that this could be accomplished for NERC posting by the week of July 20. The Chair thanked the members for their hard work together and in the subgroups and commended them on the adoption of the concept paper and the development of the announcement and comment form. The SDT adjourned at 3:00 p.m. on July 14.

I. Introductions, Agenda, and SDT Work plan Review

The Chair, Jeri Domingo-Brewer and Vice Chair, Kevin Perry welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). The SDT adopted the May 13–14 and June 17–18 meeting summary without comment or objection.

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

II. UPDATES

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

Kevin Perry made the presentation and Gerry Adamski, NERC Vice President and Director of Standards, offered additional information on behalf of Scott Mix who was not able to attend the meeting. Mr. Perry noted several areas that are under review by NERC. Mike Assante, NERC Chief Security Officer, is leading a "tiger team" with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Gerry Adamski noted that the plan to submit to NERC Board of Trustees for review and adoption at the upcoming August meeting has been delayed until the next BOT meeting in the Fall in light of the open issues and the need to clarify the implications and questions for NERC's implementation. Following its consultation with the regional entity representatives, NERC BOT hopes to adopt a final TFE process sometime next year to submit to FERC.

SDT Comments on TFEs

- Lots of questions have been raised but not yet answered.
- What are the advantages and disadvantages to NERC centrally processing all TFEs or RE's processing?
- Will TFE requests to Regional Entity be evaluated/approved or rejected in the context of CIP audits or spot check?
- Is it resolved as to whether the interim process limits TFEs to the 9 requirements? No. Proposed changes to NERC ROP (footnote 1).
- May add more requirements to list — e.g. CIP-004 R3 — personnel risk assessment.
- What role will statutory law play with the TFE? Bargaining unit agreements?
- CIP-007 R2.3 — Ports and services — document compensating measures. TFR
- CIP-007 R3.2 — Monitoring and alerts. Document compensating measures
- Submit TFE by secured means? 30 days before audit or spot check. Should they do it at point of compliance? We don't currently have a secure means yet for submission. A submittal form is under review by NERC.

- Concerns have been expressed that entities will be reluctant to submit the information on the submittal form
- TFE — remedy shortcomings and get approved if TFE rejected. Within 30 days- respond and get TFE.
- Does the violation period start when TFE rejected? NERC's intent is that the violation period begins with effective date of rejection notice but that didn't make it into the bulletin.
- There are also no penalties for frivolous filings in the current draft.
- In the proposal and interim bulletin, it doesn't cite reasons why entity could request a TFE e.g. operational, safety concerns, and conflicts with other standards.
- Is there a concern about opening up to all reliability requirements? Limit to CIP standards?
- CIP spot checks currently work with 13 requirements, none of which provide for TFE requests.
- Are pieces of TFEs covered for CIP-007? Don't have to file for that? It says "it will be documented" no TFE there now.
- The "Tiger Team" will be discussing the meaning of "where technically feasible" compliant if the entity demonstrates can't comply for technical reasons. Will there be a subset of requirements for which TFE can be received? Or will it be more open to real technical infeasibility? Lawyers are proposing tight control of the TFE.
- Some Canadian jurisdictions have issues regarding the TFE reporting through regional entities and/or NERC (e.g. Ontario). Is NERC looking to regional entities to sort through issues? If entity unsure can they work with REs vs. NERC? Should entity approach and work through RE or go through NERC directly?
- REs have presented a proposal which addresses the subject of Canadian entities. Is there an issue with submitting to NERC vs. RE? NERC expected all data on site in context with audit. Logistically and practically this won't work.
- In Ontario different frameworks been proposed about who should or not report to RE? E.g. IESO contracts. In a July 1 letter, certain entities should respond directly to the regional entity which is not currently the case. Hydro One is unclear about this. They are NERC registered entities.
- Joint regional proposal — NERC should evaluate "class type TFEs" and identify acceptable outcomes and provide for these. E.g. standards don't accommodate — field devices, anti virus etc. If we know classes of devices, we should identify acceptable alternatives to meet reliability.
- We must distinguish between interim process and long-term process.
- There is industry concern about different answers for same equipment within and across regions. The industry needs consistent methodology across all NERC regions.
- Regions are aware of this concern. They suggest the RC ask the entity to identify if other regions are being asked to address the TFE. These need the same response.
- Is our focus on interim procedures? Shouldn't we keep our eye on the longer term? Interim may look a lot like the final procedure. This will not be wasted work.

B. VSLs and VRFs

David Taylor provided an update report to the SDT on VSLs and VRFs. He noted that the SDT is making progress having developed comment forms with posting for pre-ballot review in early August. He noted that he does not expect that the SDT will need to address or deal with this going forward.

C. Update on other Related Cyber Security Initiatives

The SDT discussed the Smart Grid effort that is being led by NIST. Keith Stouffer reported on the effort led by Annabelle Lee at NIST that is addressing system level requirements from the top down and component level details from the bottom up. They are working with 800-53 NIST and ISA 99 work and are keenly aware of the work of the SDT. They have weekly telephone conferences which some members of the SDT participate and are following.

He also referenced the work now on ISA 99- Part 4 — detailed cyber security for industrial control systems. These requirements will be harmonized with other activities. They are developing their own requirements document.

Currently the categorization approach under review contains four levels of response at a system level. Next they will be developing detailed component level requirements. A proposed security compliance institute might set forth requirements which vendors can build products consistent with and have their products certified by the institute. He noted that at the upcoming ISA Expo in fall, 2009 the requirements document is scheduled to be presented for review.

Member Comments

- Is there any consideration to coordinating and synchronizing schedules and linkages among these efforts? What is the perception of the pace of the SDT's work? The perception is the SDT is not as slow as other groups.
- The Smart Grid effort is politically charged with a short time frame. Some believe the speed they are moving at will not result in effective and acceptable products.
- NIST cyber security documents are defining requirements. But what and who are the requirements to be applied to? Are they being written for those applying for DOE RFPs/grants from the $4.5 billion allocated for the smart grid? Are they also intended for those responsible with the electric grid?
- The system level requirements would apply across the whole grid — detailed cyber security requirements for different aspects of the grid. They are looking at what requirements are in the standards.
- Are there any NERC security initiatives that connect with the SDT efforts? Mike Assante will keep the SDT apprised of this.
- Nuclear initiatives? NERC alerting. Hydra — any thing needed to be known? Potential in future with hydra — BOT approved process in 2008. All procedural aspects being balloted going forward. Expedited standards development process.
- Order 706 B-Nuclear plants — how to carry forward initiatives? Development of an MOU with NRC and NERC is being developed. Development of exemption process for nuclear plants is under consideration as well as alternatives to NERC CIP umbrella under the NRC

jurisdictions. The implementation schedule for when nuclear plants held to standards is the subject of a conference call tomorrow with FERC, NERC and NRC. NERC must file by September 15, 2009, under a FERC order. NEI taken an active role on behalf of members.

- How will the process play out in terms of auditing? NERC, Regions, and NRC taking over? Permit to take more active role over auditing even though jurisdiction within NERC is still under consideration.
- NRC may a conduct audit with compliance proceeding turned over the RE.
- Looks like timeframe for proposal will dovetail with CIP Version 2 efforts. Will be handled through FERC approval of Version 2. Plants looking at Version 2 in compliance.

III. CIP-006-1 Interpretation

NERC requested that the CIP review its CIP-006-1 Interpretation. The CIP Standards Interpretation Team met the first day over lunch to reconsider the interpretation of CIP-006-1 requested by SCE&G regarding the need to physically protect Critical Cyber Assets that are dial-up accessible but do not use a routable protocol. The interpretation was previously approved by the industry but not yet submitted to the FERC for approval. The interpretation asserted that the exclusion of such Critical Cyber Assets is a correct interpretation of the standard. The FERC has questioned whether the interpretation is valid, believing that the original interpretation evaluated the Additional Compliance Information as opposed to the requirement.

The team examined CIP-002-1, CIP-005-1, and CIP-006-1, along with the FAQ for the Version 1 CIP standards and determined the following:

- CIP-006-1 contains Additional Compliance Information that was referenced in the interpretation, specifically.
- D-1.4.4 — for dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device. This additional compliance information is supported by language in the CIP-002-1 and CIP-005-1 standards and the Version 1 FAQ that clearly document the intent of the original standards drafting team.
- Put simply, the Critical Cyber Asset that does not utilize a routable protocol and is “dial-up” accessible does not have to be within an Electronic Security Perimeter per CIP-005-1, Requirement R1.2. As the CCA is not within an ESP, it is not included in protection requirement of CIP-006-1, Requirement R1.1.

While the exclusion might not have been written had the standards been developed with present day knowledge, the interpretation team agreed and the SDT concurred that the interpretation approved by the ballot body and the NERC Board of Trustees is a correct interpretation of CIP-006-1, Requirement R1.1 when viewed in the context of the complete set of Version 1 (and 2) CIP Cyber Security Standards. Any shortcomings of the requirements themselves must be remedied through standards development action.

IV. SDT Phase II — Version 3 Development Process — the “Working Paper”

A. Overview of Phase II — Version 3 Work Plan

Stu Langton reviewed the milestones in Version 2 and Version 3 of the SDT work including the work in Little Rock that framed the challenges, the subsequent development of the SDT "white papers" following the Washington D.C. meeting in December 2008 and further review and refinement of those and other papers. *(See Appendix # 5)* This resulted in the SDT convergence on a single consensus approach in Orlando that was refined further in Charlotte, Boulder City and Portland with John Lim and Phil Huff leading an expanded drafting team to continue to refine the 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 industry Members Representative Committee in May 2009. These included:

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 Portland meeting the SDT has been supplemented with additional members and BES expertise and has produced its proposed paper for the SDT's review and adoption.

B. Phase II Concept Paper Overview Presentation and SDT Adoption of the Concept Paper

On behalf of the SDT, the Chair thanked John Lim, Phil Huff and the other members of the drafting team for working productively since the Portland meeting and bringing a proposed concept paper that can be adopted by the SDT to share with the industry as the basis for the SDT's efforts in developing the Version 3 CIP-002 standards. John Lim presented the working

paper noting the significant changes that emerged from the Portland SDT meeting (*See Appendix #9).* He noted the expanded team met twice by phone and WebEx following the Portland meeting. Following the presentation, the Chair thanked the team members and others who produced an outstanding product. A motion was made by John Lim, and seconded by Phil Huff, to adopt the paper by the SDT to post for industry comment. The following member comments were offered in the discussion of the motion.

Member Comments on the Motion to Adopt the Concept Paper

- Do generation assets = networking equipment? DCS control system — switches can be critical assets. Cyber or BES consideration? Cyber consideration — more detail than the paper addresses at the conceptual level.
- Network issues = supporting SCADA communications? More detail vs. conceptual, however look at the "Target of protection" illustrations.
- Pp 12 BES subsystem e.g. Load balancing function: Plant control room- change from "center"? Guideline — control center vs. room. This was intended to reflect the same campus environment, 1 facility multiple rooms. Guidelines as a "room"(s).
- SDT agreed to change control centers to "room(s).
- Contingency reserve section. Any units company has 150 mw? This is done by hardware — shared groups multiple owners of same equipment.
- What level trying to drive at? 150 mw? Not looking at individual units. 10 150 mw in a plant.
- How can we head off and deal with the industry "CIP-002-009 mentality?" Will there be a mountain of documentation for every digital asset? Every digital asset in BES and everything it talks to as well? Everything will now be at least a "low."
- How will we handle industry comments back on the concept? Is the SDT bound to all aspects of the concept paper? The SDT should consider the concept paper as complete and out for industry comment. The input on the concept paper will help the SDT as it develops CIP-002-009 standards and requirements going forward.
- The SDT should consider the lessons learned in the CIPC guidelines approach. The comment form was structured to ask the industry to comment on particular issues. This approach could directly facilitate efforts for the SDT to use the input as the process goes forward
- The SDT should work today and tomorrow to develop a clear and structured comment form for the concept paper.
- Important to convey that this is a "big picture concept approach" signaling the direction of changes from previous versions in terms of approach (vs. Version 1 and 2). The cover letter/announcement will be crucial in setting the stage.
- Make sure the concept paper has Reference line numbers and invites suggestion.
- Will there be an opportunity for industry to say maybe this is too much? Yes.
- Concerns with the idea that this paper will never see a character changed in it is overblown. These tend to become reference archived documents. We should clarify to the industry that the SDT will not mount concerted effort to respond to every comment and seek to adjust the

concept paper accordingly. But as we develop the requirements and address industry concerns, we can update the concept paper as appropriate.

- We have to do a selling job on both concept paper and standards themselves. We need to convince the industry that this is the right approach. While this may look to the industry to be onerous, in reality it will be easier, more consistent, easier to comply with standards over the longer term. The industry will build upon, not lose the work they have put into the CIP to date.
- We need to consider as we write requirements how the entity can demonstrate compliance with the requirement. Today it is an exercise with mountains of paperwork. We should try to address this as we go forward.
- Concept Paper will be archived as a background document. Address comments by incorporating responses in the first draft of CIP-002 requirements.
- The concept paper has provided a visual representation of our ideas. Agree that industry is wary of documents.
- Jackie Collett offered to take a look at the concept paper with the "Queen's" English in mind. The chair accepted the offer.
- The SDT needs to let industry know we are making progress. We should be prepared to present at the NERC October 14–15 Dallas workshop this approach as a "paradigm shift" in cyber security.

Following the discussion the SDT unanimously adopted the concept paper as revised for sharing with the industry and agreed to develop a draft of a comment form for the paper.

The team discussed a "game plan" for communications with the Industry on the working concept paper and agreed to the following steps:

1. Post in July the Working Concept Paper for Comment and Suggestions (with a cover and comment form with key questions to be developed on July 14 by the subgroups and the SDT);
2. Presentation of the concept paper to MRC on August 4, 2009;
3. Webinar(s) to the Industry in August 2009; and
4. Presentation of the industry comment and SDT progress at NERC Workshop on Compliance and Cyber Security (October 14–15, 2009)

V. Development of Concept Paper, Draft Announcement, and Comment Form

On the second day the SDT agreed to develop a draft announcement and comment form. Each of the 5 subgroups was asked to draft questions for the industry to respond to in each of their areas. The SDT believed this would help to solicit industry comments that the sub-groups could use in developing draft requirements. The Chair, with assistance of staff drafted an announcement and cover letter for the paper which was reviewed, refined, and adopted by the SDT. (*See Appendix #11*) The subgroups presented their draft questions to the SDT which offered suggestions. The subgroups then redrafted their questions and the SDT adopted the following for use in the comment form to be posted with the concept paper:

Reliability Functions

1. Is the concept of the categorizing by function instead of by asset clear? If not why?
2. The BES Reliability Functions listed in the "BES Function" column of the table were not meant to be comprehensive. Are there any others functions we need to address and why?

BES Subsystems and BES Cyber Systems

1. Does the methodology presented in the Identification of BES Subsystems and the Identification of BES Cyber Systems sections capture all of the systems that will need to be protected to achieve an acceptable level of reliability? What other issues need to be considered?

BES Mapping

1. The concept paper proposes that all identified BES subsystems are mapped into categories based on pre-defined criteria which reflect their impact on the reliability and operability of the BES: this mapping will be based on pre-defined criteria in the functions they provide or support, which determine the level of that impact. Do you agree with this approach and if not, what alternative suggestions do you have?
2. The paper gave an example of High, Medium and Low impact levels. What do you believe is the appropriate number of levels for impact mapping of the BES subsystems?
3. Do you prefer discrete thresholds or performance based criteria for mapping BES sub-systems? E.g. MW values as opposed to percentage of total generation. Please explain.

Cyber Analysis

1. Section X.X, Categorization of Cyber Systems, describes how an entity determines the impact a specific Cyber System has on to its assigned BES reliability functions. Do you agree with this process described in the concept paper? Please explain.
2. Section X.X, Final Categorization of Cyber Systems Based on Overall Impact on the BES, describes an example process of how an entity combines the BES impact mapping and Cyber System impact analysis to determine the overall impact a Cyber System has on the BES. Do you agree with this process described in the concept paper? Please explain.
3. Section X.X, Defining the Target of Protection, describes how an entity determines the set of Cyber Assets necessary to provide security assurance in the BES functions the Cyber System performs. Do you agree with this process described in the concept paper? Please explain.

Definition and Selection of Controls

1. Provide your company's thoughts on applying different levels of protection (i.e. security controls) based on characteristics and impact categories of specific BES cyber systems (e.g. transmissions substations, generating plants, control centers) as discussed in Section XX of the concept paper.
2. Section XX of the paper introduces the concept of a library of security controls:
    a. What sources would you recommend the drafting team consider when developing a library of security controls for protecting categorized BES cyber systems?

b. What specific challenges would you anticipate in implementing controls from among a library of security controls?

The SDT agreed that the Chair will oversee the final agreed upon edits to the adopted concept paper, announcement, and comment forms. She indicated she would circulate it to the members for one last look later in the week and then work with NERC to post it for an industry comment period the week of July 20.

VI. CIP-002 SUBGROUPS

A. Introduction, Organization, Appointment and Charge to the CIP-002 Subgroups

In advance of the meeting the Chair and Vice Chair circulated to members a proposal for the work plan from July–December, 2009. The Chair reviewed the proposal which set forth roles and responsibilities and included involving all members of the SDT in at least one of five proposed subgroups to develop draft requirements for consideration by the SDT to be included in a draft CIP-002 Version 3. Through SDT Subgroups and the full SDT, an initial draft of CIP-002 requirements and measures would be produced by December 2009 consistent with the Working Paper concepts and consensus points. In the fall of 2009, the SDT would begin initial drafting of the standards that will replace the current versions of CIP-003 through CIP-009 in parallel with the CIP-002 posting and balloting. In 2010 the SDT would respond to industry comments and post the new CIP-002-009 for balloting later in 2010-2011.

Building on the Working Paper, the following topical SDT subgroups were proposed and agreed to by the SDT to develop an initial set of CIP-002 requirements:

1. Reliability Functions
2. List of BES Subsystems and/or BES Cyber Systems
3. BES Mapping
4. Cyber Analysis
5. Definition and Selection of Controls (sample control or set of controls from the controls catalogue as a “proof of concept”).

Each SDT member present ranked, in order of preference, their interest in participating in each of the 5 subgroups. (*See Appendix #7*). In light of preferences, the Chair and Vice Chair proposed the following composition for the 5 working groups:

Subgroup Name	Members and Observers
Reliability Functions	John Varnell (1), Jim Brenton (1), Dave Norton, Rich Kinas, Doug Johnson, James Bassett
List of BES Subsystems and/or BES Cyber Systems	Jackie Collett, Scott Rosenberger, Jay Cribb, and Gerry Freese.
BES Mapping	John Lim (1), Jeri D. Brewer (1), Dave Revill (2)

	Sharon Edwards and Kevin Sherlin
Cyber Analysis	Chris Peters, Phil Huff , Rob Antonishen, Frank Kim and Joe Doetzl. Sam Merrell and Mike Toecker
Definition and Selection of Controls	Kevin Perry, Bill Winters, Jon Stanford, Keith Stouffer. Peter Schneider

On the morning of day two, Stu Langton presented some tips and guidelines for the subgroup leaders and members on small group discussion and shared leadership. *(See, Appendix 10)*

B. Subgroup Organizational Meetings and Comment Form Questions

On the afternoon of the first day the 5 groups met in parallel organizational sessions to: review scope of topic and identify areas that may need development of related CIP-002 requirements; determine what information they will need going forward; select a leader/spokesperson, a scribe and a timekeeper; sketch out a work plan, including meetings, to get the work done by the October SDT meeting. Subgroups reported back at the end of day one and day two the issues they identified and their plans going forward.

1. Reliability Functions Subgroup

This subgroup agreed that John Varnell will serve as the subgroup lead and Jim Breton would serve as the subgroup scribe and Rich Kinas would perform the timekeeper role. They agreed to the request of James Basset, IPS and Doug Johnson, Commonwealth Edison to help with the subgroup's work. They met both the first and second day of the meeting. John reported the group will plan on meeting weekly starting with July 20 and use WebEx and offered the following report on their work:

Purpose: Define Reliability Functions for new CIP-002-3 (Version 3) NLT Oct 2009 Meeting

Members attending (July 13) in Vancouver, BC: John Varnell, Chair, Jim Brenton, EROCT, Secretary, Rich Kinas, Sgt at Arms/Time keeper, Dave Norton, not in Conf call (may be on bench) James Bassett, IPS, Observer Doug Johnson, Commonwealth Edison

Schedule: Weekly Meetings — WebEx and conference calls — Richard Kinas (set first WebEx for July 20 at 9 a.m. CDT)

Goals and Objective: Fully defined basic reliability functions prior to the October SDT meeting using key inputs from those who have not been previously involved with team efforts(Observers: Doug Johnson (NERC OC member) and James Basset). Need to provide list of key Reliability Functions to BES Mapping Group ASAP

Needed Resources: Review functions:

- Executive Summary of Paper and ALRs (from the CA Guidelines),
- Version 4 and 5 Functional Model,
- Draft Working Paper, and
- Reliability Functional Model Technical Document,

- CA and CCA Identification Guidelines.

Initial Activity:
ID functional model elements needed for reliability--Then break down for each Functional Entity.

Major Activities reported to Full Team

1) Set schedule to discuss weekly with key team of members and observers — Done
2) Structured organization — John Leads, Jim types, Rich watches as timekeeper and Sgt at Arms
3) Collect and distribute Five key documents to all team members — Done

Out of Scope: We may not be able to develop Detailed Requirement Specs since this is a structural segment of the overall model, and does not lend itself to detail requirement specification TBD with John Varnell.

Concept Paper Comment Form Questions regarding Reliability Functions

- Is the concept of the categorizing by function instead of by asset clear? If not why?
- The BES Reliability Functions listed in the "BES Function" column of the table were not meant to be comprehensive. Are there any others functions we need to address and why?

2. List of BES Systems/BES Cyber Systems Subgroup
Jackie Collett is the Subgroup lead, Jay Cribb will serve as scribe and Scott Rosenberger will serve as timekeeper and Gerry Freese will serve as a member.

The Subgroup met on both days and reported to the SDT the following 10 key questions they will be exploring in developing their recommendations:

a) We need definitions and requirements from other standards that apply (Contingency Reserve, etc). Will the BES Reliability group be providing these?
b) How do we handle systems that cross functional model entities?
c) What is the definition of "system"? (This is foundational).
d) Will there be minimum criteria to be on the lists?
e) What is the methodology for identifying BES assets and cyber assets?
f) How do we limit the cyber assets included in 'connections'? What are the boundary conditions for BES systems/cyber systems?
g) How do we handle the dynamic nature of the grid and the BES systems/assets? Example: Contingency Reserve is a MW threshold and the units designated for it may change often.
h) What is "common mode failure"? It is used several times in the white paper.
i) How do we handle controls at the 'perimeter' vs. controls on every 'inside' asset/component?
j) What is the proper granularity of "system" identification?

Concept Paper Comment Form Questions regarding List of BES Subsystems

- Does the methodology presented in the Identification of BES Subsystems and the Identification of BES Cyber Systems sections capture all of the systems that will need to be protected to achieve an acceptable level of reliability? What other issues need to be considered?

3. BES Mapping Subgroup

John Lim will serve as leader, Sharon Edwards as scribe, Dave Revill (as timekeeper), Kevin Sherlin and Jeri Domingo Brewer as members. They reviewed and agreed on the subgroup's scope as primarily defining criteria/ numerical thresholds. They noted they needed input from the reliability function subgroup and they would need to address overlap and coordination as their output is our input. In terms of Impact level (for example, DHS tiers) the subgroup will define the number of levels that will be used.

The subgroup brainstormed the following:

- Review DHS Critical Asset Tiers, NERC Event Classification Criteria, NERC Critical
  - Other documents may help us including the DHS Critical Tiers
  - NERC Event Classification Criteria — guidance for people to classify events
  - NERC Critical Asset Guideline
  - Guideline for Critical Cyber Asset identification
- Asset Risk Assessment Guide
- Other NERC Reliability Standards
- Get input from our own shops as to their level of support for the various concepts and thresholds

The subgroup agreed to meet once per week in the near term on Wednesdays at 3 p.m. EST. The next meeting would be on August 5 from 3 to 5 p.m. by phone. Also the group will meet early for the August drafting team meeting at 1 p.m. on the day prior, which is August 19, face to face at a meeting place TBD.

Assignments for subsequent meeting: Take the DHS and the BES and CA Guideline and get comments from the operating groups.

The group developing the following initial input/questions for the comment form which were reviewed by the SDT with suggestions for refinements and consolidation:

- Would the industry prefer criteria for minimum thresholds & then the industry can define whether they want to do more?
- Please provide your thoughts on the appropriate thresholds to establish criticality.
- Does your company support numeric thresholds for categorizing generation?
- Does your company support numeric thresholds for categorizing substations?

- Does your company support a numeric threshold for categorizing control centers?
- The paper proposes a categorization of all BES assets
  - Do you support this concept?
  - Why or why not?
- The paper proposes categories based on pre-defined criteria
  - Do you support this approach?
  - If not, what alternative method do you suggest?
- What do you believe is the appropriate number of levels for categorization of the BES assets?
- Do you have other suggestions for categorization of assets?

Following their presentation to the SDT, the subgroup refined and consolidated a proposed list of 3 questions:

Concept Paper Comment Form Questions regarding BES Mapping

- The concept paper proposes that all identified BES subsystems are mapped into categories based on pre-defined criteria which reflect their impact on the reliability and operability of the BES: this mapping will be based on pre-defined criteria in the functions they provide or support, which determine the level of that impact. Do you agree with this approach and if not, what alternative suggestions do you have?
- The paper gave an example of High, Medium and Low impact levels. What do you believe is the appropriate number of levels for impact mapping of the BES subsystems?
- Do you prefer discrete thresholds or performance based criteria for mapping BES sub-systems? E.g. MW values as opposed to percentage of total generation. Please explain.

4. Cyber Analysis Subgroup

Phil Huff will serve as leader, Chris Peters as scribe, and Rob Antonishen as timekeeper, Frank Kim and Joe Doetzl will serve as members. Sam Merrell and Mike Toecker will participate as observers. The subgroup will seek to address "defining the target of protection" and dealing with 3rd party interconnections. The reported on the following issues to the SDT:

- Interconnections — how to address of about cyber assets- functional perspective or within controls.
- Lots of interface with security controls in terms of what the impact categories will be, how many levels we need and interface with the selection of controls.
- Risk analysis in selecting controls. Look at how to implement risk assessment to replace the TFE process, work with controls group. Somewhere between cyber analysis and controls

In the discussion of the report one members urged the subgroup to keep in mind that the standards process needs to produce measurable requirements which may be challenges to do in the context of risk analysis.

Concept Paper Comment Form Questions regarding Cyber Analysis

- Section X.X, Categorization of Cyber Systems, describes how an entity determines the impact a specific Cyber System has on to its assigned BES reliability functions. Do you agree with this process described in the concept paper? Please explain.
- Section X.X, Final Categorization of Cyber Systems Based on Overall Impact on the BES, describes an example process of how an entity combines the BES impact mapping and Cyber System impact analysis to determine the overall impact a Cyber System has on the BES. Do you agree with this process described in the concept paper? Please explain.
- Section X.X, Defining the Target of Protection, describes how an entity determines the set of Cyber Assets necessary to provide security assurance in the BES functions the Cyber System performs. Do you agree with this process described in the concept paper? Please explain.

5. Definition and Selection of Controls Subgroup

Keith Stouffer will serve as Subgroup leader and they will employ floating scribes and timekeepers among the members: Kevin Perry, Bill Winters and Jon Stanford. Peter Schneider will participate as an observer. They discussed how best to organize the controls framework. Should it be the same as the CIPS have; or the 27001, NIST framework, or the ISA 99 framework? They agreed to work on keeping the current CIP structure and framework but propose collapsing Standards 005 and 007 into a single standard. They will use work from ISA 99 and 853 and map them into a CIP structure. They agreed to work with 3 levels of security controls. Keith noted that the subgroup hopes to have a strawman of the control set done for SDT review by the next SDT meeting in August in Charlotte.

They will take current ISA 99 foundational requirements and start looking at samples of controls for examples. They hope to show examples of low, moderate and high to demonstrate to the industry how it will work and what it will change. The subgroup will work by email between meetings.

Concept Paper Comment Form Questions regarding Definition and Selection of Controls

- Provide your company's thoughts on applying different levels of protection (i.e. security controls) based on characteristics and impact categories of specific BES cyber systems (e.g. transmissions substations, generating plants, control centers) as discussed in Section XX of the concept paper.
- Section XX of the paper introduces the concept of a library of security controls:
    - What sources would you recommend the drafting team consider when developing a library of security controls for protecting categorized BES cyber systems?
    - What specific challenges would you anticipate in implementing controls from among a library of security controls?

C. Subgroup Roles, Responsibilities, Coordination and Guidelines

The SDT discussed the roles that would be played by SDT members, subgroup members, subgroup leaders a coordinating team and staff.

On the second day the SDT agreed that it would be helpful to develop a set of coordination guidelines for the subgroups and suggested:

- Each subgroup should create its own email distribution list to share documents and ideas
- When a subgroup is ready to issue something to the SDT PLUS List, the subgroup leader will send it electronically to Joe Bucciero and he will send it out to the SDT PLUS List.
- Subgroups are expected to meet and coordinate their activities between SDT Meetings. Each subgroup leader will work with the Coordinating Group between SDT Meetings to report on progress and ensure coordination among the 5 subgroups.

VII. NEXT STEPS AND CLOSING

The Chair reviewed with the SDT the schedule for getting the concept paper, the announcement and comment form finalized and posted on the NERC website for industry comment. She suggested this could be accomplished by the week of July 20.

The Chair thanked the members for their hard work together and in the subgroups and commended them on the adoption of the concept paper.

The Chair noted that she and Kevin appreciated and thanked on behalf of the SDT the Drafting Group members for an outstanding job in bringing the SDT to consensus on the concept paper.. Members completed an onsite meeting evaluation form *(See, Appendix #3).*
The SDT adjourned at 3:00 p.m. on July 14.

APPENDICES TABLE OF CONTENTS

Appendix 1: Meeting Agenda 20

Appendix 2: Meeting Attendees List 22

Appendix 3: Meeting Evaluation Summary 24

Appendix 4: NERC Antitrust Guidelines 26

Appendix 5: SDT Work plan Schedule 28

Appendix 6: CIP-002 Work plan Proposal 31

Appendix 7: CIP-002 Subgroup Assignments 33

Appendix 8: SDT Version 3 Points of Consensus- April, 2009 35

Appendix 9: Working Paper: Categorizing Cyber Assets: An Approach Based on BES Reliability Functions 36

Appendix 10: Herding Cats 101Tips for Small Group Discussion and Shared Leadership 38

Appendix 11: Draft Announcement-Concept Paper, July 14, 2009 39

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

Monday, July 13, 2009 | 8 a.m.–5 p.m. PDT
Tuesday, July 14, 2009 | 8 a.m.–5 p.m. PDT
Vancouver, B.C. Canada

Proposed Meeting Objectives and Outcomes

- Receive update on TFE and VSL/VRF processes;
- Review, refine, and adopt the CIP Version 3 Working Paper as a conceptual framework going forward;
- Test SDT consensus on the NERC Request for Response for Interpretation CIP 006-1;
- Agree on SDT 002 Drafting Subgroups organization;
- Convene SDT 002 Drafting Subgroups organizational sessions and report back to SDT; and
- Agree on next steps and assignments.

Monday July 13, 2009

1. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**
   - Roll Call; NERC Antitrust Compliance Guidelines
   - Facilitator review of May 13–14 Boulder City, NV meeting summary and adoption; and
   - Facilitator review of June 17–18 Portland, OR meeting summary and adoption
2. **Review of Meeting Objectives, Agenda, and Meeting Guidelines — Jeri Domingo Brewer, and Bob Jones**
3. **Update on Technical Feasibility Exception NERC Rules of Procedure — Scott Mix**
4. **Update on VSLs and VRFs — David Taylor**
5. **Update on Other Related Cyber Security Initiatives — SDT Members**
6. **Overview of Steps to Date in the CIP Version 3 (Phase 2) Development Process — Stu Langton**
7. **CIP Version 3 Categorizing Cyber Systems Working Paper — Presentation — John Lim, Phil Huff et al**
8. **Key Outstanding Issues — John Lim, Phil Huff et al**
9. **Proposed CIP-002 Subgroup Process-Members Complete Preference Forms**
10. **Working Lunch — Convene SAR Interpretation Team to Review possible Responses to NERC on Interpretation of CIP 006-1**
11. **Review SAR Interpretation Team Proposed Response to NERC Request for Interpretation of CIP-006-1**
12. **CIP Version 3 Working Paper — Resolve Any Key Issues — John Lim, Phil Huff et al**
13. **Test Consensus and Seek Adoption of the Working Paper for Industry Review**

14. **Review SDT Communication Plan — MRC Meeting, Posting Paper for Comment (14 days), SDT Webinar, Comment Period (30 days)**
15. **Review CIP-002 Work Plan Proposal and Proposed Subgroups and Membership**
16. **Adjourn**

Tuesday July 14, 2009

1. **Welcome and Agenda Review — Jeri Domingo-Brewer**
2. **Summary of Day One Outcomes — Bob Jones**
3. **Subgroup Protocols — Herding Cats 101 — Stu Langton**
4. **Organizational Sessions of the CIP-002 Subgroups — Small Group Breakouts**
5. **CIP-002 Drafting Group Reports and SDT Input — Plenary Session**
6. **Next Steps and CIP Version 3 Process and Work Plan — Review Proposed 2010 Meeting Schedule**
7. **Review Charlotte August Meeting Objectives**
8. **Meeting Evaluation**
9. **Adjourn**

Appendix # 2

Attendees List
July 13–14, 2009 Vancouver, BC

Attending in Person — SDT Members

1. Rob Antonishen	Ontario Power Generation
2. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
3. Jim Breton	ERCOT
4. Jackie Collett	Manitoba Hydro
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff	Arkansas Electric Coop Corporation
8. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
9. Frank Kim	Ontario Hydro
10. Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, Southwest Power Pool
11. Christopher A. Peters	ICF International
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy
14.Keith Stouffer	National Institute of Standards & Technology
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
16.William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	NERC
3. Joe Bucciero	NERC/Bucciero Assoc.
4. David Taylor	NERC
5. Gerry Adamski	NERC
6. Robert Jones	FSU/FCRC Consensus Center (Wed. & Thursday)
7. Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via WebEx and Phone

17. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
18. Rich Kinas	Orlando Utilities Commission
19. Sharon Edwards	Duke Energy
20. Kevin Sherlin	Sacramento Municipal Utility District
21. Jonathan Stanford	Bonneville Power Administration

Others Attending in Person

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

Others Attending via WebEx and Phone

James Bassett	Lafayette
Mark Braendle	ABB
Mark Grace	
Doug Johnson	ConEd
Travis Jeffery	
Kim Long	Duke
Jerry Mannerino	
Mike Mertz	SCE
Hoang Ngo	RI Eng
Nitin Patel	
Mike Sanders	SoCal
Robin Siewart	EON

Appendix # 3 — Meeting Evaluation Feedback Summary

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

1) **Please assess the overall meeting.**
   9.14 The agenda packet was very useful.
   8.29 The pre-meeting papers (White Paper and Process Evaluation Summary) were very useful.
   7.33 The WebEx document display and the audio were effective
   7.21 The quality of the meeting facility was good.
   9.29 The objectives for the meeting were stated at the outset.
   9.50 Overall, the objectives of the meeting were fully achieved.
   Were each of the following meeting objectives fully achieved:
   9.29 Receive update on TFE and VSL/VRF processes;
   9.29 Review, refine and adopt the CIP Version 3 Working Paper as a conceptual framework going forward;
   9.30 Test SDT Consensus on the NERC Request for Response for Interpretation CIP 006-1;
   9.29 Agree on SDT 002 Drafting Subgroups organization;
   8.93 Convene SDT 002 Drafting Subgroups organizational sessions and report back to SDT; and
   8.67 Agree on next steps and assignments.

2) **Please tell us how well you believe the Team members and participants engaged in the meeting.**
   8.93 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
   9.14 The Facilitators made sure the concerns of all members were heard.
   9.07 The Facilitators helped clarify and summarize issues.
   7.73 The Facilitators helped members build consensus.
   7.93 The Facilitators made sure the concerns of all participants were heard.
   8.43 The Facilitators helped us arrange our time well.

3) **What is your level of satisfaction with what was achieved at the meeting?**
   9.07 Overall, I am very satisfied with the results of the meeting.
   8.36 Overall, the design of the meeting agenda was effective.
   8.93 I was very satisfied with the services provided by the Facilitators.
   9.00 I am satisfied with the outcome of the meeting.
   9.29 I know what the next steps following this meeting will be.
   9.43 I know who is responsible for the next steps.

4) **Other comments:**
   What did we achieve?
   - Approved concept paper; organized for development of requirement language.
   - White paper is done
   - Approving the whitepaper provided a basis for moving forward.
   - Sub group, updates, scheduling.
   - Approval and concept paper

   What are our biggest challenges going forward?

- Moving along the same path
- Industry consensus
- V3, control development
- Moving concepts to reality through requirements. Maintaining group involvement in a recession.
- Keeping sub group momentum.
- Achieved drafting so COP 002- Approval to catalog of controls.

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

- Set up earlier to start on schedule
- Better facilities for subgroup meetings. Internet access for everyone.
- Continue levering sub groups.
- Problems with room on 1st day could have been better resolved.

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

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

III. Activities That Are Permitted

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

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

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

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

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

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

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

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

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

APPENDIX # 5
Meeting Schedule
October 2008–December 2010

Development of CIP Version 2 and Version 3 Framework

October 2008–July 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 Version 3 process reviewed.

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

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed Version 3 white papers.

January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

March 2–April 1, 2009 — 30-day Pre Ballot

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

March 30, 2009 — WebEx meeting(s) White Paper Drafting Team

April 1–10 — NERC Balloting on Version 2 Products

April 6, 2009 — WebEx meeting — White Paper Drafting Team

April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call

April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx

April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.

June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

June — WebEx meeting(s)

- Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria

CIP-002 Development of Requirements, Measures, Etc. July-December 2009

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

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

July–August Interim WebEx meeting(s)

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

August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**

Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.

13. August 20–21, 2009 in Charlotte, NC

- SDT Plenary session to review and respond to MRC input on Working Paper/CIP-002 Concepts
- SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper

NERC Webinar

August–September Interim WebEx meeting(s)

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

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

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

September–October Interim WebEx meeting(s)

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

15. October 20–22, 2009 in New Orleans, LA

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

October–November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–18, 2009 in Tampa, FL

- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.

November–December Interim WebEx meeting(s)

- Drafting teams as needed to finalize drafts
- CIP-002 Coordination Team meeting

17. December 15–17, 2009 in Atlanta, GA

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

Refinement of CIP-002 and Development of Other CIP Standards

January–December 2010

(12 SDT monthly meetings and subgroup WebEx meetings as needed)

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

Proposed 2010 Meeting Schedule

January 20–21 — Wednesday–Thursday	July 14–15, Wednesday–Thursday
February 17–18 — Wednesday–Thursday or February 16–18 — Tuesday–Thursday	August 11–12, Wednesday–Thursday
March 10–11 — Wednesday–Thursday or March 9–11 — Tuesday–Thursday	September 8–9, Wednesday–Thursday
April 14–15 — Wednesday–Thursday or April 13–15 — Tuesday–Thursday	October 13–14, Wednesday–Thursday or October 12–14
May 12–13 — Wednesday–Thursday	November 17–18, Wednesday–Thursday
June 9–10 — Wednesday–Thursday or June 9–11 — Tuesday–Thursday	December 15–16, Wednesday–Thursday

Appendix # 6
Project 2008-06 Cyber Security Order 706 SDT CIP-002 Work plan Proposal — July 2009

A. CIP-002 Work plan Objectives

1. Establish the overall schedule and milestones for developing the new CIP reliability standards on cyber security
2. Involve all members of the SDT in at least one of five proposed subgroups to develop draft requirements for consideration by the SDT to be included in a draft CIP-002 Version 3.
3. Present the SDT Working Paper (Categorization of Cyber Systems) to the NERC Member Representative Committee at its August 2009 meeting.
4. Post, host a webinar, and receive and consider industry comments on the Working Paper in August-September 2009 as the SDT drafts CIP-002 Version 3.
5. Through SDT Subgroups and the full SDT, produce an initial draft of CIP-002 requirements and measures by December 2009 that are consistent with the Working Paper concepts and consensus points.
6. Seek and respond to industry comment and post the new CIP-002 for balloting in 2010
7. Begin initial drafting of the standards that will replace the current versions of CIP-003 through CIP-009 in parallel with the CIP-002 posting and balloting.
8. Prepare and issue the replacements for CIP-003 through CIP-009 for posting and balloting in 2010/2011.

B. Proposed CIP-002 Subgroups

Building on the Working Paper, the following topical subgroups are proposed to develop an initial set of CIP-002 requirements:

1. Reliability Functions
2. List of BES Subsystems and/or BES Cyber Systems
3. BES Mapping
4. Cyber Analysis
5. Definition and Selection of Controls (sample control or set of controls from the controls catalogue as a "proof of concept").

C. Proposed Steps for Forming CIP-002 Subgroups- Vancouver

1. On day one, ask each SDT member to rank in order of preference their interest in participating in each of the 5 subgroups. In light of preferences, propose composition for the 5 working groups with 3-6 members in each.
2. On day two, convene the 5 groups in parallel and ask members to: 1) review scope of topic and identify areas that may need development of related CIP-002 requirements; 2) determine what information they will need going forward; 3) select a leader/spokesperson, a scribe and a timekeeper; 4) sketch out a work plan, including meetings, to get the work done by the October SDT meeting. Subgroups will report back their plans on Day 2 of the Vancouver Meeting to the SDT.

3. Where possible, provide staff /facilitator support for the subgroups.
4. Follow up with SDT members not attending the Vancouver meeting for team placement, as needed.

D. Roles and Responsibilities

1. **CSO706 SDT Members.** Review, build consensus, and adopt a draft CIP-002 by December 2009. Members will also begin parallel development efforts in 2010 to draft the new standards that will eventually replace the current CIP-003 through CIP-009 standards once the requirements and measures for the new CIP-002 standard have been defined and vetted.

2. **CIP-002 Subgroup Members.** Subgroup members will be responsible for producing a draft set of requirements related to their topic prior to the October 20-22 SDT meeting. Subgroup members will be responsible for selecting a leader/spokesperson, a scribe and a timekeeper.

3. **CIP-002 Subgroup Leaders.** The Leader will be responsible for leading and facilitating the subgroup's effort in creating and implementing a plan (deliverables, timeline, assignments, review and consideration of industry comments) in consultation with members and with help, as needed, by staff and facilitators.

4. **CIP-002 Coordinating Team.** The SDT Chair and Vice Chair along with the Subgroup Leaders and facilitators will participate on a Coordinating Team that will meet by conference call in advance of each monthly SDT meeting through October 2009 to address any duplication of tasks, identify needs for coordination among the subgroups and vetting of the approaches being considered by each of the subgroups to help smooth the way for preparation of a complete draft of CIP-002 to be reviewed, refined, and adopted in November and December 2009.

5. **Staff and Facilitation Support.** Where/when needed and/or requested, facilitation or other staff support will be provided to the subgroups.

Appendix # 7 — SDT Member Subgroup Assignments

Subgroup Name	Members and Observers
Reliability Functions	John Varnell (1), Jim Brenton (1), Dave Norton, Rich Kinas, Doug Johnson, James Bassett
List of BES Subsystems and/or BES Cyber Systems	Jackie Collett, Scott Rosenberger, Jay Cribb, and Gerry Freese.
BES Mapping	John Lim (1), Jeri D. Brewer (1), Dave Revill (2) Sharon Edwards and Kevin Sherlin
Cyber Analysis	Chris Peters, Phil Huff, Rob Antonishen, Frank Kim and Joe Doetzl. Sam Merrell and Mike Toecker
Definition and Selection of Controls	Kevin Perry, Bill Winters, Jon Stanford, Keith Stouffer. Peter Schneider

Subgroup Preference Form

(Jeri DB, Chris P, Keith s, Jay C, John L., Jim Breton, John Varnell, Dave Revill, Kevin P, Phil H, Rob A., Bill W. Jackie Collett , Jon Stanford, Dave Norton, Scott R, Frank Kim

No forms: Rich Kinas, Sharon Edwards, Gerry Freese, Kevin Sherlin,

Reliability Functions
Potential members: **John Varnell (1), Jim Brenton (1), Dave Norton,**

[Preferences: JDB (5) CP (4) KS (5) JCr (5) JL (3) **JB (1) JV (1**) DR (5) KP (5) PH (5) RA (5) **JC (2)** JS (5) DN SR (5) FK (5)]

List of BES Subsystems and/or BES Cyber Systems

Potential members: **Jackie Collett (1), Scott Rosenberger (1), Jay Cribb (2) (Sharon Edwards), (Gerry Freese)**

[Preferences: JDB (3) CP (5) KS (3) JCr (2) JL (4), JB (5) JV (3) DR (4) KP (4) PH (4) RA (4) JC (1) JS (5) DN, SR (1) FK (3)]

BES Mapping
Potential members: **John Lim (1), Jeri D. Brewer (1), Dave Revill (2) (Rich Kinas)**

[Preferences JDB (1) CP (3) KS (4), JCr (4) JL (1) JB (4) JV (2) DR (2) KP (2) PH (3) RA (2) JC (3) JS (5) DN SR (5) FK (4)]

Cyber Analysis

Proposed members: **Chris Peters (1), Phil Huff (1), Rob Antonishen (1), Frank Kim (1) (Kevin Sherlin)**

[Preferences: JDB (2), CP (1) KS (5) JCr (3) JL (2) JB (2) JV (5) DR (3) KP (3) PH (1) RA (1) BW (2) JC (4) JS (3) DN, SR (2) FK (1)]

Definition and Selection of Controls
Proposed members: **Kevin Perry (1), Bill Winters (1), Jon Stanford (1), Keith Stouffer (1)**

[Preferences: CP (2) KS (1) JCr (1) JL (5) JB (3) JV (4) DR (1) KP (1) PH (2) RA (3) BW (1) JC (5) JS (1)
JDB (4) DN, SR (3)]

Appendix # 8
Version 3 SDT Points of Consensus — April 16, 2009

A. The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems.

B. The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.

C. The Standard's BES Impact Assessment will consider a categorization process.

D. 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.

E. 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.

F. 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.

G. The Standards will provide Organizations with reasonable flexibility in applying equivalent security controls on the basis of compensating controls and environmental considerations.

H. The Standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.

I. The Standards will state explicit criteria for the BES Impact Assessment.

J. The Standards will state explicit criteria for the Cyber Impact Assessment (including use and misuse of cyber systems).

K. The Standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 9 — 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

07/15/2009 — Team

TABLE OF CONTENTS

CATEGORIZING CYBER SYSTEMS: AN APPROACH BASED ON IMPACT ON BES RELIABILITY FUNCTIONS Error! Bookmark not defined.

EXECUTIVE SUMMARY .....**Error! Bookmark not defined.**

INTRODUCTION .....**Error! Bookmark not defined.**

BES RELIABILITY FUNCTIONS .....**Error! Bookmark not defined.**

IDENTIFICATION OF BES SUBSYSTEMS .....**Error! Bookmark not defined.**

CATEGORIZATION OF BES SUBSYSTEMS .....**Error! Bookmark not defined.**

THIRD PARTY OVERSIGHT OF BES SUBSYSTEMS AND THEIR CATEGORIZATION .....**Error! Bookmark not defined.**

IDENTIFICATIOn OF ESSENTIAL CYBER SYSTEMS .....**Error! Bookmark not defined.**

CATEGORIZATION OF CYBER SYSTEMS.....**Error! Bookmark not defined.**

CYBER SYSTEM INTERCONNECTIONS .....**Error! Bookmark not defined.**

EXTERNAL CYBER SYSTEM DEPENDENCIES.....**Error! Bookmark not defined.**

FINAL CATEGORIZATION OF CYBER SYSTEM BASED ON OVERALL IMPACT ON THE BES .....**Error! Bookmark not defined.**

DEFINING THE TARGET OF PROTECTION.....**Error! Bookmark not defined.**

APPLYING SECURITY CONTROLS TO THE TARGET OF PROTECTION.....**Error! Bookmark not defined.**

CONCLUSION .....**Error! Bookmark not defined.**

APPENDIX A: TERMS AND DEFINITIONS .....**Error! Bookmark not defined.**

Appendix #10
Herding Cats 101
Some Tips on Small Group Discussion and Shared Leadership

Purposes:

- Increase Member Participation
- Idea-Creation
- Problem-Solving, Product-Development
- Consensus-Building

Needs:

- Adequate Time
- Leadership
- Right-Size, Right-Composition
- Right Space/Technology, Connecting with others
- Full member engagement and active listening

Some Tips for Leaders and Members:

1. Clarify purpose, tasks, and end results (products/outcomes)
2. Select leaders to organize, chair, keep-records of discussion and proposals, keep-time
3. Create a timed agenda/schedule (get group input, review, and agreement)
4. Identify challenges regarding issues or tasks
5. Identify shared values and principles to guide
6. Use questions to guide (and get them right)
7. Involve everyone in discussion and work
8. Review/summarize discussions frequently and re-clarify question/task
9. Stimulate discussion (brainstorm, nominal group process, strawman drafts, etc.)
10. Use visuals to communicate and connect ideas
11. Connect with absent members
12. Be evaluative (review decisions, processes, and performance).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #11 — Working Concept Paper Draft Announcement 7-14-09

July XX, 2009

TO: INDUSTRY STAKEHOLDERS

RE: **REQUEST FOR INFORMAL SUGGESTIONS AND COMMENTS REGARDING THE CONCEPTS CONTAINED IN THE CSO 706 SDT WORKING CONCEPT PAPER "CATEGORIZING CYBER SYSTEMS AN APPROACH BASED ON BES RELIABILITY FUNCTIONS"**

Ladies and Gentlemen:

In 2008, FERC Order 706 paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) need for ERO guidance regarding the risk-based assessment methodology; (2) scope of critical assets and critical cyber assets; (3) internal, management, approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order 706. The SDT began meeting in October, 2008.

The SDT believes the CIP-002 standard and requirements provide a foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After months of deliberation, the SDT is considering an approach to CIP-002 that identifies and categorizes critical assets and critical cyber assets according to impacts on reliability functions. This approach is outlined in the attached draft working paper, *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*.

The Team seeks informal industry feedback and suggestions on the concepts presented in the attached draft working paper. The SDT seeks suggestions and comments particularly regarding four areas set forth in the draft working paper: BES Reliability Functions; Identification of BES subsystems and/or BES Cyber systems; BES Mapping; Cyber Analysis. The informal industry feedback will be considered by the SDT in developing CIP-002 draft requirements. A draft CIP-002 standard will be posted for formal industry comment as part of the ANSI standards development process later this year.

The concepts presented in the draft working paper, propose a broader and more comprehensive cyber security approach to protect the systems that support a reliable BES. The draft working paper deals primarily with the identification and classification of BES assets and cyber systems.

The SDT has provided a form for industry participants to offer their informal suggestions and comments on the concepts in the draft working paper.

Suggestions and Comments Due: September 1, 2009