NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

April 14, 2009 | 1–5 p.m. EST
April 15, 2009 | 8 a.m.–5 p.m. EST
April 16, 2009 | 8 a.m.–noon EST
Charlotte, North Carolina

Meeting Summary Contents

Cover *1*
Contents *2*
Executive Summary *3*

I. Introductions, Agenda Review and Review of SDT Workplan 7

II. Technical Feasibility Exception Update and SDT Discussion 7

III. VSL and VSR SDT Discussion 8

IV. Phase I Industry Comment/SDT Response Document Review 8

V. Review of Media and Congressional Treatment of Cyber Security Issues 9
A. NERC's Response 9
B. Representative Markey's Letter to FERC 10
C. SDT Communication Efforts Going Forward: "A Key Messages Task Group" 11

VI. SDT 706 Phase II White Paper Review and Discussion 12
A. White Paper Review *John Lim, Phil Huff, et al* 12
B. Review of SDT Phase II Consensus Points 13

VII. Next Steps 17
A. 2009 Workplan Approach 17
B. Workplan Schedule 17
C. White Paper Development 17
D. Meeting Evaluation 18

Appendix 1: Meeting Agenda 19
Appendix 2: Meeting Attendees List 21
Appendix 3: NERC Antitrust Guidelines 23
Appendix 4: SDT Workplan Schedule 25
Appendix 5: Congressman Markey's Letter to FERC 27
Appendix 6: White Paper: Categorizing Cyber Assets: An Approach Based on BES Reliability Functions 29

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

EXECUTIVE SUMMARY

Joe Bucciero conducted a roll call of members and participants, the Chair reviewed the meeting objectives and the facilitator, reviewed with the team and participants the proposed meeting agenda.

Mr. Bucciero reviewed with the team the need to comply with NERC's Antitrust Guidelines. The team reviewed and unanimously adopted on March 12 the SDT February 18–19, 2009 meeting summary. Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for both Phase 1 and Phase 2 development. At the conclusion of the meeting the SDT agreed on a schedule of meetings from July–December, 2009. The team reviewed and unanimously adopted on April 16 the SDT March 10–12, 2009 meeting summary.

Scott Mix, NERC staff, provided an update on the TFE process. He indicated that he is aware that EEI has indicated it will be filing comments. Once the comments are in, NERC's legal staff and leaders will address the comments. He believes the comments will be addressed and the document will be sent to the NERC board for approval in the summer of 2009. After NERC board approval, the modification to the NERC Rules of Procedure for the TFE will be sent to FERC for approval and filed with the appropriate Canadian governmental authorities.

Dave Taylor, NERC staff, provided an update on VSL/VSR process. FERC issued a recent order on two standards. FERC said in their order that it was not sure about the use of a 'roll-up' approach to VSLs. FERC asked that NEC provide further explanation of the approach. The VSLs proposed for CIP-002 through CIP-009 have included some of these roll-up VSLs embedded in them. He noted that the there may to be a future reassessment if FERC doesn't allow for this approach.

During a pre-session on Tuesday morning, a team, lead by Kevin Perry, prepared responses to the comments received in the ballot of CIP Version II. The SDT reviewed each of the draft responses, suggested changes and reached consensus on all of the responses by Thursday morning. Some of the major issues contained in the comments were:

- Comments concerning the constrictive nature of the Technical Feasibility Exception Process;
- Designation of the Senior Manager as overly prescriptive;
- Objections to the inclusion of "continuous" monitoring in CIP-006 for physical security;
- Several commented and expressed concerns on the reduction from 90 days to 30 days for changes to be made in the standards.

The group reviewed Kevin Perry's initial draft, refined and finalized the team responses to the comments made after the posting of CIP Version II to the industry. The team unanimously adopted the Response Document (16-0) as revised on Thursday morning and asked Kevin Perry with assistance from Joe Bucciero to finalize the document for submission to NERC and to initiate the recirculation ballot.

The team discussed the publicity and media stories last week regarding the vulnerability of the electric grid raising concern with the hyperbole (characterizing as “Pearl Harbor”, “Hiroshima”, “9/11”) and lack of evidence for many of the claims. A letter from Representative Markey, House Homeland Security to FERC and draft legislation filed by Senators Rockefeller and Snow were noted.

Michael Assante, NERC’s Chief Security Officer, provided the team with a briefing on NERC’s response to the media coverage of the last week beginning with the Wall Street Journal article. He noted that NERC has sought to strike the right tone in a complex area of policy and practice. NERC worked behind the scenes with press, congress, FERC and industry associations and issued a press statement noting that the industry is committed to working hard on cyber security and the SDT effort to develop new standards is a leading example of this effort. While acknowledging the reality of continuing vulnerability, NERC challenged the notion that there was evidence of any cyber security compromises that have adversely affected reliability. He noted NERC is working with industry associations. He suggested SDT has a role to play and that it shouldn’t be seeking to defend the industry. NERC will be trying to get the message out as to the progress to date and the SDT role in addressing cyber security and reliability.

Gerry Freese made a proposal made to put together a comprehensive presentation that might be given to Congressional staffers to get out the message that the industry is taking cyber security seriously and has made great efforts. In addition the message would explain some of the inaccuracies contained in the recent publicity concerning vulnerabilities of the electric grid. Facilitators suggested that the briefing for congress might be created in conjunction with the update. In general team members supported a message responding to the recent publicity. The Chair suggested the SDT form a “Key Messages Task Group” and solicited members who would want to participate: Gerry Freese agreed to lead the effort, and John Stanford, Jerry Domingo Brewer, Jay Cribb, Dave Norton, Phil Huff, Rich Kinas and Jim Breton all agreed to participate.

Mr. Langton, SDT facilitator, reviewed the significant progress the team has made together since October 2008. He then set the stage by saying that the point of the Phase II Concept paper presentation is to assure SDT member understanding of the concept and invite ideas for strengthening and clarifying aspects of the concept.

John Lim introduced the white paper noting contributions from Jackie Collett, Bill Winters, Phil Huff and assistance from Scott Mix in refining the white paper since the March SDT meeting in Orlando. He noted the group met two times by phone and WebEx, and convened a SDT WebEx meeting and met this morning. They agreed that they needed additional input and contributions from other SDT members in developing the concept paper. He also noted that the group will need to define terms used in the document. One change in the approach is to move away from a “risk assessment” to an “impact based assessment.” He offered the following overview of the concept:

- Identification and categorization of BES Assets.

- Identification of the cyber systems that support functions or BES assets.
- The idea is to combine the two categorizations to supply the categorization for the asset.
- All applicable cyber assets (EMS, substation, relay, etc.) will need to be identified with a categorization level.
- Total impact on the BES system will need to be determined using the table.
- The categorization will then be utilized for the requirements that follow.

Following a review and discussion of each section of the paper the facilitator asked if any of the SDT members had any fundamental difficulty with the approach and then polled the SDT members as to whether all were comfortable at the conceptual level with the current white paper approach. All members agreed to go forward indicated that they liked the direction the white paper was taking. All acknowledged that they would continue to test this as the details were developed.

On day two, John Lim and Phil Huff agreed to draft some general draft consensus points from the white paper that could be presented by the Chair to the NERC Members Representative Committee on May 4, 2009. They were joined by Jackie Collett, Scott Rosenberg, John Varnell and Rich Kinas. The SDT reviewed and refine these on Thursday morning resulting the following 11 points which received a 3.8 of 4 rank in terms of their acceptability. The chair agreed to base her presentation on the points:

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 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 mis-use 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.

The Chair also agreed to put these points in a narrative format for a letter to Mike Assante as part of the SDT's input to NERC as it develops its input to FERC in response to Rep. Markey's letter.

Bob Jones, SDT facilitator presented the concept of CIP-002- requirements and measures being the work undertaken for the rest of 2009 with the goal of posting for industry comments on a complete CIP-002 standard and go to ballot on it. This might include taking a requirement from CIP-003 through CIP-009 to illustrate how CIP-002 would related to the later development of CIP-003 through CIP-009. The SDT would then develop the entire CIP-003 through CIP-009 package and post for comments and balloting as a complete package. The schedule proposes that the SDT will be into 2012 when a full version of CIP version III is posted for comments.

The Chair reminded people to register for the Boulder City meeting and that the September meeting would take place in Folsom, California near Sacramento and not in Denver:

The CIP-002 sub team will continue working on the parts of the white paper that need development. Categorization of the BES assets still needs refinement and help. The sub team asks for assistance from outside the group. Scott Mix will take the lead to see if additional expertise can be provided to the sub team.

The team offered an evaluation regarding what was accomplished, what helped and what might help for the future.

The Chairman concluded the meeting concluded by thanking the host (Duke Energy) and is looking forward to hosting the meeting in Boulder City. The SDT adjourned at 11:45 a.m. on April 16.

I. Introductions, Agenda Review and Review of SDT Workplan

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

Mr. Bucciero reviewed with the team the need to comply with NERC's Antitrust Guidelines *(See, Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion. The team reviewed and unanimously adopted on April 16th the SDT March 10–12, 2009 meeting summary.

Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for both Phase 1 and Phase 2 development. (*See Appendix #4)* The Chair noted that the meeting location in September would be changed from Denver to Sacramento or Folsom, California. The facilitators noted that the team may want to adjust the work plan so that it is clear that when the Phase II White Paper is ready for release, it will be done so by informally posting on the NERC Web site, inviting industry reactions without triggering the need for a formal ANSI step. This will enable the team to focus in on the development of CIP-002 for potential posting by the end of the calendar year.

Mr. Langton noted that by the conclusion of the meeting, the SDT needed to have the responses to the industry comments completed and sent to NERC for posting and to begin the recirculation ballot and to have made progress on the Phase II white paper and approach.

II. Technical Feasibility Exception Update and SDT Discussion

Scott Mix, NERC staff, provided an update on the TFE process. He indicated that he is aware that EEI has indicated it will be filing comments. Once the comments are in, NERC's legal staff and leaders will address the comments. He believes the comments will be addressed and the document will be sent to the NERC board for approval in the summer of 2009. After NERC board approval, the modification to the NERC Rules of Procedure for the TFE will be sent to FERC for approval and filed with the appropriate Canadian governmental authorities. The modification to the NERC Rules of Procedure becomes effective after regulatory approvals. Scott noted that NERC staff will not be provided individual responses to each comment. See, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

III. VSL and VSR Committee Update

Dave Taylor, NERC staff, provided an update on VSL/VSR process. FERC issued a recent order on two standards. FERC said in their order that it was not sure about the use of a 'roll-up' approach to VSLs. FERC asked that NERC provide further explanation of the approach. The VSLs proposed for CIP-002 through CIP-009 have included some of these roll-up VSLs

embedded in them. He noted that the there may to be a future reassessment if FERC doesn't allow for this approach.

Mr. Taylor noted that VRF (violation risk factors) must be assigned to each requirement and any sub requirement. The team that was working on these assigned the VSL's at the requirement level, rather than at each sub requirement level. Therefore, the VSL's for the CIP standards that have been created may have to be un-wound and applied at the sub requirement level. See http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

IV. Phase I Response Document Review

During a pre-session on Tuesday morning, a team, lead by Kevin Perry, prepared responses to the comments received in the ballot of CIP Version II. The SDT reviewed each of the draft responses, suggested changes and reached consensus on all of the responses by Thursday morning. Some of the major issues contained in the comments were:

- Comments concerning the constrictive nature of the Technical Feasibility Exception Process;
- Designation of the Senior Manager as overly prescriptive;
- Objections to the inclusion of "continuous" monitoring in CIP-006 for physical security; and
- Several commented and expressed concerns on the reduction from 90 days to 30 days for changes to be made in the standards.

The group reviewed Kevin Perry's initial draft, refined and finalized the team responses to the comments made after the posting of CIP Version II to the industry. The team unanimously adopted the Response Document (16-0) as revised on Thursday morning and asked Kevin Perry with assistance from Joe Bucciero to finalize the document for submission to NERC and to initiate the recirculation ballot. For the final response document see: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

V. Review of Media and Congressional Treatment of Cyber Security Issues

The team discussed the publicity and media stories last week regarding the vulnerability of the electric grid raising concern with the hyperbole (characterizing as "Pearl Harbor", "Hiroshima", and "9/11") and lack of evidence for many of the claims. A letter from Representative Markey, House Homeland Security to FERC and draft legislation filed by Senators Rockefeller and Snow were noted.

A. NERC's Response

Michael Assante, NERC's Chief Security Officer, provided the team with a briefing on NERC's response to the media coverage of the last week beginning with the Wall Street Journal article. He noted that NERC has sought to strike the right tone in a complex area of policy and practice. NERC worked behind the scenes with press, congress, FERC and industry associations and issued a press statement noting that the industry is committed to working hard on cyber security and the SDT effort to develop new standards is a leading

example of this effort. While acknowledging the reality of continuing vulnerability, NERC challenged the notion that there was evidence of any cyber security compromises that have adversely affected reliability. He noted NERC is working with industry associations.

He suggested the SDT has a role to play and that it shouldn't be seeking to defend the industry. NERC will be trying to get the message out as to the progress to date and the SDT role in addressing cyber security and reliability.

Member Comments:

- Someone needs to set the media straight on the facts.
- Why not securing the whole infrastructure. What about water, etc.
- External communication plan for SDT not for the industry.
- Need to distinguish between securing and complying?
- Better standard does not imply better security. It is not the be-all-end-all.
- NIST as a dismal failure in federal systems?
- As a vendor, 85% of the approach that electric industry clients want to know: how do I get around this?
- If you look at other industries, their public relations efforts are far more effective. Our industry is doing good things and making a valuable contribution but the industry woefully poor in blowing it own horn.
- Standards with a compliance focus give leverage for IT/cyber managers to get things done right. Tool and level for security. Tell our story.
- Need some communication. CIP standards 1 part of puzzle. NERC alerts and Mike Assante. Not necessarily spokesman for cyber security.
- Need to show we are making progress. Need to get on board on Phase III. Need to establish consensus.
- NERC has been relatively quiet. It appears that NERC gets the industry to do things because they are forced to. The standards should be directed towards getting people on the right path to a secure grid.
- If we and industry don't come forward with reforms, Congress will tell us exactly how to do it and we will not like it.
- Impact Assessment= just the consequences. Technical impact- cyber impact- (level of access and results of exploit) BPS impact- impact of effect of denied or compromised
- Concerned that we seemed focused on external threats and system level compromises. Cyber threats much larger. This may reinforce fear and alarmism related to threats to BPS.
- Insider threats, physical threats. E.g. the NIST family of controls- 17 control areas and none have to do with this type of threat.
- What the venue would be to expand the scope- other aspects of security that don't fit cleanly into matrix?
- How to categorize- e.g. technical impact- other forms of attack that may not be categorized. More inclusive in terms of other forms.

- We would do well in our analysis to first assume the worst case scenario- will that result in BPS impact on that cyber assets. Open breakers, etc. What is the worst that can happen?
- If this is for rapid assessment it will be ok. If this is for the longer term it could confuse the industry.
- Breakthrough- work from planning for the worst possible thing- bad or stupid guy from the inside, bad from outside. Later do a care and feeding. Figure out what problem we are solving. Care and feeding and prevention- handled in 03-009. 002 scope, what do I need to do, how much and where.
- NIST standards- like the simplicity. Little more than wording.
- Matrix doesn't take into account the compromise of one leading to stepping up to others and affect the whole system.
- BPS impact side- operating security event level.
- Make sure the likelihood of the impact is reality based. What are components of BES we need to spell out. What are things we have seen that are likely to happen we should focus on. Flushing out BPS impact.
- General sentiment- useful but content may not be appropriate for what we are trying to do.

B. Representative Markey's letter to FERC

On April 9, 2009 Rep. Edward J. Markey (D-Mass.), Chairman of the House Energy and Commerce Committee Subcommittee on Energy and the Environment, sent a letter to FERC regarding the escalating cyber breaches threatening to compromise the electricity grid. NERC is preparing a set of responses to FERC for their consideration in responding to Representative Markey. Mike Assante welcomed the SDT suggestions for NERC's input to FERC.

Member Comments

- Who loaded their gun on this?
- NERC hopes FERC sets the context. The standards piece is just a part of a greater whole in terms of responding to Congress. Minimum standards- uniformly across system because you are interconnected.
- Standards were to provide a "comprehensive…"
- Care taken in addressing the 3rd bullet. "implementing"
- Compliance enforcement piece; spot checks and audits are beginning-
- CERP started audits last fall on the 13 requirements. Midwest ISO.

C. SDT Communication Efforts Going Forward — A "Key Messages Task Group"

Gerry Freese made a proposal made to put together a comprehensive presentation that might be given to Congressional staffers to get out the message that the industry is taking cyber security seriously and has made great efforts. In addition the message would explain some of the inaccuracies contained in the recent publicity concerning vulnerabilities of the electric grid. Facilitators suggested that the briefing for congress might be created in conjunction

with the update. In general team members supported a message responding to the recent publicity.

Member Comments

- Take advantage of some industry presentation opportunities upcoming and coordinate the message: e.g. Jon Stanford is participating on a RSA Panel? Mike Assante on a RSA panel.
- Don't think about the industry as a monolith. Break it up. Deal with different pieces. 3200 organization in NA half with no SCADA system at all.
- Analysis — 160 systems with a profile of interest to terrorists. Spending time and money on security that doesn't work.
- Cannot stop professional hackers — we put up "honey pots" to trip them up. Operational military networked hacked. Gene Spafford testified before Rockefeller until improve quality we will have problems. Until we get the stuff built into the products, its going to be
- We should be getting congressional staffers together organized, structured, where we are, where we have been. Briefing. If materials prepared, Mike Assante offered to gather staffers. Timing is critical, should happen within 1-2 months.
- In terms of the discussion in DC, there is willingness to hear this message. We should strike while the iron is hot.
- Toiling in anonymity — the public and congress only getting 1 side of the picture.
- We should use all approaches (briefings, conference presentations, press coverage) as vehicles. Premier security event. Opportunity.
- Do we need have professionals help us in shaping the message? We can use some our best industry corporate communications. Concern about "misshaping the message." We should guard against not too much outside influence.
- Staff briefings can help dialogue and discussion.

The Chair suggested the SDT form a "Key Messages Task Group" and solicited members who would want to participate: Gerry Freese agreed to lead the effort, and John Stanford, Jerry Domingo Brewer, Jay Cribb, Dave Norton, Phil Huff, Rich Kinas and Jim Breton all agreed to participate.

VI. SDT Phase II CIP 002 White Paper Review and Refinements

Mr. Langton, SDT facilitator, reviewed the significant progress the team has made together since October 2008 including completing Phase I and agreeing conceptually on a thoughtful mix of CIP and NIST approaches to Phase II. He noted that additional SDT members will need to assist and contribute to the development of the Phase II White Paper. He then set the stage by saying that the point of the Phase II Concept paper presentation is to assure SDT member understanding of the concept and invite ideas for strengthening and clarifying aspects of the concept.

A. Phase II White Paper Review

John Lim introduced the white paper noting contributions from Jackie Collett, Bill Winters, Phil Huff and assistance from Scott Mix in refining the white paper since the March SDT meeting in Orlando. He noted the group met two times by phone and WebEx, convened a SDT WebEx meeting and met this morning. They agreed that they needed additional input and contributions from other SDT members in developing the concept paper. He also noted that the group will need to define terms used in the document. One change in the approach is to move away from a "risk assessment" to an "impact based assessment." He offered the following overview of the concept:

- Identification and categorization of BES Assets.
- Identification of the cyber systems that support functions or BES assets.
- The idea is to combine the two categorizations to supply the categorization for the asset.
- All applicable cyber assets (EMS, substation, relay, etc.) will need to be identified with a categorization level.
- Total impact on the BES system will need to be determined using the table.
- The categorization will then be utilized for the requirements that follow.

R1 — Identification of BES Assets

Member comments

- How will this be done?
- The SDT goal should be to create a set of criteria that are specific enough to characterize BES assets.
- Did David Taylor/NERC have a concept paper on this point? Scott Mix noted a paper was prepared but upon review was not sufficiently on point.
- There were several questions for the small group that was putting this paper together. Several in the group had questions around the role of the planning assessments in determining categorization of BES assets.
- The group answered that planning engineers will need to be involved, but those details had not all been worked out. The group asked for volunteers from SDT members who have planning engineering background.
- Need Power system engineers and transmission planners to assist in this part of the concept. Perhaps people like John Sykes who briefed the SDT in Phoenix?
- Jason Marshall, Midwest ISO volunteered to assist in this effort

R2 — Critical Asset Identification Method
R3 — Critical Asset Identification
R4 — Cyber Asset Identification
R5 — Categorization of Cyber Assets

Member comments

- There was much discussion about the use of RTO's and/or RC's for oversight of the categorization.

- The group also questioned the oversight process and whether that would be done by the RC function or by the regions of NERC. A team member explained that RC's, RTO's, etc. may not want to oversee the process and categorization due to liability concerns.

R6 — Annual Approval

Member comments

- What about third party oversight? Third party oversight is provided for in the whitepaper as was specified in FERC Order 706.

Member final comments on the Concept

- Need to acknowledge that the way the SDT is working is different.
- We need to address all sections of the white paper and stay at a fairly high level.
- We know we have agreement. Address shortcomings of the current system.
- Cover all the BES assets not just the critical — categorize all.
- Cover all relevant cyber systems related to BES assets.
- The focus on reliability of functions.
- 5 major points list. Short paragraph on each to enable Jerry fields questions. Enough
- Does this build on principles and on industry investments?
- Flexibility is important

The facilitator asked if any of the SDT members had any fundamental difficulty with the approach and then polled the SDT members as to whether all were comfortable at the conceptual level with the current white paper approach. All members agreed to go forward indicated that liked the direction the white paper was taking. All acknowledged that they would continue to test this as the details were developed.

B. Phase II Consensus Points — Preparing for the Member Representative Committee Presentation

On day two, John Lim and Phil Huff agreed to draft some general draft consensus points from the white paper that could be presented by the Chair to the NERC Members Representative Committee on May 4, 2009. They were jointed by Jackie Collett, Scott Rosenberg, John Varnell and Rich Kinas. The SDT agreed to review and refine these on Thursday morning.

Below is the initial draft and strikethrough/underlined following the SDT discussion.

1. **The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems. ~~The Standards will require a BES impact assessment as opposed to risk based assessment.~~**

   Member Comments

   - Drafters intended this as a "soft ball."

- Didn't have the criteria to do a risk based assessment.
- "As an approach to Risk based assessment."?
- Standards "will"? The proposed version "will seek to"?
- Concerned about the removal of risk based in #1
- Agree. the standards will incorporate ~~be primarily~~ ~~based solely on~~ a BES impact assessment. Include a BES impact assessment in lieu of a risk based assessment.
- If keep in, consider "instead of a primarily risk based assessment"
- CIA- risk management is also an accepted lexicon.
- Members agreed with changes reflected above.

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

   Member Comments
   - None, ok

3. **The Standard's BES Impact Assessment will ~~include categorizing~~ consider a categorization process ~~all BES assets~~**

   Member Comments
   - If you categorize "all", will still come up with equivalences
   - Uncomfortable with "all" Haven't defined at what level we are going to categorize. "More" vs. "all"? Delete "all"
   - Categorize now as critical and non critical. Flag each asset or classes
   - "categorize all BES assets"?
   - "More categories"
   - Will each have some security requirements associated with it?
   - Will consider including more categories than we have today.
   - "risk" or "impact" categories. Impact level categories than previous versions of CIP
   - Will include a categorization process.
   - Members agreed with changes reflected above.

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.**

   Member Comments
   - None, ok

5. **The Standards will categorize ~~and apply security requirements (or controls) to all~~ 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. ~~**The standards will require Entities to apply security controls to Cyber Systems commensurate and appropriate to their potential impact on the BES.**~~

Member Comments

- "All"?
- Categorize requirements "to those systems."?
- Members agreed with changes reflected above.

6. **The final Cyber System categorization will reflect the impact to the BES based on a** ~~**security incident i.e.**~~ **loss of availability** ~~**confidentiality,**~~ **integrity,** ~~**and/or**~~ **confidentiality** ~~**availability**~~ **of the Cyber System.**

   Member Comments

   - Shows how we are going to do the categorization.
   - "Loss of confidentiality"?
   - Standard lexicon — remove reference to "incident" CIA standards order
   - Switch confidentiality to last and availability to first?
   - Data confidentiality is a concern.
   - Cyber system — impact of cyber assets if compromised. Doing a translation from power engineering and cyber engineering side of the house. Need to be understood by the multiple disciplines.
   - Military is focused on confidentiality and that was the primary driver of the early models.
   - If take off table, we are presupposing it is not important.
   - "As appropriate?
   - Data and system integrity? Common understanding? Normal understanding includes.
   - The order doesn't matter.
   - Data applied to system only? No. we have background check requirements.
   - Members agreed with changes reflected above.

7. **The Standards will provide Organizations with reasonable flexibility** ~~**should have reasonable flexibility**~~ **in applying equivalent security controls on the basis of compensating controls and environmental considerations.**

   Member Comments

   - Members agreed with changes reflected above.

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

   Member Comments

- Members agreed with changes reflected above.

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

   Member Comments
   - Missing criteria for the cyber impact assessment? Add an additional point.
   - Use and misuse of cyber assets
   - This is concept not detailed idea.

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

    Member Comments
    - Members agreed with adding the new point reflected above.

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

    Member suggestions for the MRC presentation
    - Use the flow chart to present
    - Use diagrams where possible to illustrate the concept.
    - Keep in mind that MRC mostly senior mgrs VP- markets,
    - A participant on the phone suggested the SDT consider the following language as part of the consensus point, "Seek to have more understandable, streamlined with fewer cross references, clearer set of standards." The chair noted these consensus points were to present to the MRC the sense of the SDT on how they agreed to go forward for Phase II standards development. She noted the language suggested may or may not reflect the sense of the SDT at this point. The facilitator suggested that the comment would be included in the meeting summary.

Acceptability Ranking Scale	4 = acceptable, I agree	3 = acceptable, I agree with minor reservations	2 = not acceptable unless major reservations addressed	1 = not acceptable	Avg.
Consensus Points	**10 (5/5)**	**2**	**0**	**0**	**3.8 of 4**

The Chair will base her MRC presentation on these consensus points. She will also put these points in a narrative format for a letter to Mike Assante as part of the SDT's input to NERC as it develops its input to FERC in response to Rep. Markey's letter.

VII. Workplan, White Paper, Meeting Evaluation and Next Steps

A. 2009 SDT Workplan Approach

Bob Jones, SDT facilitator presented the concept of CIP-002- requirements and measures being the work undertaken for the rest of 2009 with the goal of posting for industry comments on a complete CIP-002 standard and go to ballot on it. This might include taking a requirement from CIP-003 through CIP-009 to illustrate how CIP-002 would relate to the later development of CIP-003 through CIP-009. Scott Mix noted that it would be important to get CIP-002 to industry ahead of consideration of the catalogue of controls. The SDT would then develop the entire CIP-003 through CIP-009 package and post for comments and balloting as a complete package. The schedule proposes that the SDT will be into 2012 when a full version of CIP version III is posted for comments.

Phil Huff noted that Bill Winters suggested NIST has done a lot of work on guidelines. The SDT may want to dedicate a future meeting to get input and cooperation from those experts familiar with implementing NIST. John Varnell reminded team members that Keith Stoffer, John Stanford and Jeri Brewer were on the team to bring that perspective.

B. Workplan Schedule

The Chair reminded people to register for the Boulder City meeting and that the September meeting would take place in Folsom, California near Sacramento and not in Denver.

Proposed Dates and Locations for Future Meetings 2009

Dates in 2009	Location
April 14–16	Charlotte
May 13–14	Boulder City, NV
June 17–18	Portland
July 13–14	Toronto
August 20–21	Chicago
September 9–10	Folsom, California
October 20–22	New Orleans
November 17–18	Atlanta
December 15–17	Tampa (FRCC)

C. CIP 002 White Paper Development.

CIP 002 White paper development: The sub team will continue working on the parts of the white paper that need development. Categorization of the BES assets still needs refinement and help. The sub team asks for assistance from outside the group. Scott Mix will take the lead to see if additional expertise can be provided to the sub team.

D. Meeting Evaluation — What worked and what could be improved?

Wireless connectivity has turned out to be an expectation of the group. On the final day of the Charlotte meeting, connectivity was intermittent for some members.

What did the SDT accomplish?

- Got through recommendations and responses to industry comments to enable the recirculation ballot.
- Identified the need for communication within and beyond the industry.
- Made a big step forward in consensus on the principles to be included in the white paper.

What things helped us to accomplish these?

- Strawman documents are very helpful — e.g. Kevin's response document.
- Getting facilitators to the meeting.
- Having a quorum.
- Having the WebEx stay up.
- Continued open engagement and attention of all SDT members.
- Silence is golden consent rule worked well.

What suggestions are there for the future?

- Periodically spend about 30 minutes brainstorming future concepts/ideas that may become topics for future white papers.

The Chairman thanked the host (Duke Energy) and is looking forward to hosting the SDT meeting in Boulder City. The SDT adjourned at 11:45 a.m. on April 16.

Appendix # 1 — Meeting Agenda

April 14, 2009 | 1–7 p.m. EST
April 15, 2009 | 8 a.m.–7 p.m. EST
April 16, 2009 | 8 a.m.–noon EST
Duke Office — Conference room number 2313
400 South Tryon St
Charlotte, NC

Proposed Meeting Objectives and Outcomes

- Receive updates on TFE and VSL processes
- Receive a briefing on the NERC Critical Assets Industry Survey
- Review and Draft Responses to Phase I Industry Comments
- Review and Refine Phase II Framework White Paper
- Agree on assignments and next steps in the SDT Work plan.

Tuesday, April 14, 2009

1. Phase II White Paper Team Drafting Session
2. Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry
    a. Roll Call
    b. NERC Antitrust Compliance Guidelines
    c. Review and adoption of March 10-12, 2009 Meeting Summary
3. Review of Meeting Objectives, Agenda and Meeting Guidelines — Jeri Domingo and Bob Jones
4. Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton
    - Review of April-December 2009 SDT Schedule
5. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting — Scott Mix
6. Update on VSL/VSR for Version 1 and 2 CIP-002-009 — David Taylor
7. Overview of SDT Phase II Development Process Steps and CIP 002 Review — Stu Langton
8. Critical Assets Industry Survey — Mike Assante
9. CIP-002 White Paper Presentation — Bill Winters and Jackie Collett
10. Q & A and Discussion and Initial Consensus Testing
11. Break
12. Phase I Small Group Proposal for Response Drafting
13. Small Groups Draft Responses to Industry Comments
14. Break — If Needed, Small Groups may continue working until 7:00 p.m.
15. Recess

Wednesday, April 15, 2009

1. Welcome, Agenda Review and Roll Call

2. Phase I Small Group — Draft Responses to Industry Comments
3. Break
4. Phase I Small Group — Draft Responses to Industry Comments
5. Working Lunch
6. Small Group Reports and SDT Review and Consensus Testing of Draft Responses
7. Break
8. Small Group Reports and SDT Review and Consensus Testing of Draft Responses
9. Break — If Needed, Full or Small Groups may continue working until 7:00 p.m.
10. Recess

Thursday, April 16, 2009

1. Welcome, Agenda Review, and Roll Call
2. CIP-002 White Paper Consensus Testing
3. Break
4. CIP-002 White Paper Consensus Testing
5. Review of May SDT Agenda and Objectives
6. Meeting Evaluation — What Worked, What Could be Improved?
7. Adjourn

Appendix #2 — Attendees List for March 10–12, 2009 Meeting in 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. Sharon Edwards	Duke Energy
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
8. Frank Kim	Ontario Hydro
9. David Norton	Policy Consultant, CIPEnergy Corporation *(Tues & Wed.)*
10. **Kevin B. Perry, Vice Chair**	Director, IT-Infrastructure, Southwest Power Pool
11.Keith Stouffer	National Institute of Standards & Technology
12. John D. Varnell	Technology Director, Tenaska Power Services Co.
1. Roger Lampilla	*NERC*
2. David Taylor	*NERC (Tuesday)*
3. Scott R. Mix	*NERC*
4. Tom Hoffstetter	*NERC (Formerly Midwest ISO, Inc)*
4. Joe Bucciero	*NERC/Bucciero Assoc.*
6. Robert Jones	*FSU/FCRC Consensus Center (Wed. & Thursday)*
7. Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

13. Jackie Collett	Manitoba Hydro
14. Joe Doetzl	
15. Phillip Huff	Arkansas Electric Coop Corporation
16. Richard Kinas	Orlando Utilities Commission
17. Scott Rosenberger	Luminant Energy
18. Kevin Sherlin	Sacramento Municipal Utility District
19. Jonathan Stanford	Bonneville Power Administration

SDT Members Unable to Attend

1. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
2. Christopher A. Peters	ICF International
3. David S. Revill	Georgia Transmission Corporation
4.William Winters	Arizona Public Service, Inc.

Others Attending in Person

Jim Breton	ERCOT
Travis Jafray	Subnet Solutions
Jason Marshall	Midwest ISO
Darren Highfill	ENERNEX
Sam Morrell	CERT

Others Attending via WebEx and Phone

Chris Wright	
James Bassett	Lafayette
David Huff	FERC
Bob Tallman	E.ON
Chris Wright	Burns & Mac
Raghu Rayalu	SCE (Wed.)

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

Participants in NERC activities (including those of its committees and 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 #4
January–December Draft Project Schedule (Revised April 2009)

OVERVIEW

- **13 SDT Face-to-Face Meetings**
- **Multiple SDT subgroup and subcommittees WebEx Meetings**
- **One Cyber Expert and Stakeholder Workshop (**Summer/Fall 2009 — Tentative)
- **Industry Comments on CIP-002 SDT White Paper** (June–July 2009)
- **2 NERC Members Representative Committee Meetings,** (May & August 2009)

SDT Draft Schedule — January-December 2009

1. **January 7–9 Meeting in Phoenix, AZ** (half, full, half day format Wednesday–Friday)
   - Review of Technical Feasibility Exceptions white paper
   - Review of Industry Comments on Phase 1 products — Establish and convene small groups to draft responses
   - Review of Phase 2 White papers

January 15 WebEx meeting(s)
- Small group draft responses to industry.

January 21 WebEx meeting(s)
- Small group draft responses to industry.

2. **February 2–4 Meeting in Phoenix, AZ** (half, full, half day format Monday–Wednesday)
   - 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 I and Phase I Product Revisions.

3. **February 18–19 Meeting in Fairfax, VA**
   - Update on Phase I process
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review, discussion and refinement of Phase II and CIP-002 White papers, strawman and principles

4. **March 10–11 Meeting in Orlando, FL** (half, full, full day format)
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review and Refinement of Phase II 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 — Phase I Ballot Results and Industry Comments

5. **April 14–16 Meeting in Charlotte NC** (half, full, half day format Wednesday–Friday)
   - Update on NERC TFE process
   - Update on VSL Team process
   - Update on the NERC Critical Assets Survey
   - Review in SDT small groups and respond to Phase I Ballot Results and Industry Comments
   - Review and Refinement of Phase II Whitepaper and Progress Report to MRC

May 4 — Member Representative Committee Meeting in Arlington, VA — SDT progress report.

6. **May 13–14 Meeting in Boulder City NV** (2-day format Wednesday–Thursday)
   - Review MRC presentation and any input to SDT on Phase II white paper
   - Further SDT refinement of the strawman Phase II White Paper in plenary and small groups.

7. **June 17–18 Meeting in Portland OR** (2-day format)
   - Further SDT refinement and adoption of the Draft Phase II White Paper for industry comment.
   - Review potential SDT subcommittee structure and work plan for implementation of Phase II.

~~**Industry Comment Period on SDT Phase II White Paper- 45 days** (June 20-August 5, 2009)~~

8. **July 13–14 Meeting in Toronto, ON**
   - Agree on and charge subcommittees and conduct organizational meetings
   - SDT Subcommittees meet to organize and begin drafting revisions to CIP and/or addressing assigned issues.
   - Subcommittee organizational reports to SDT

July–August WebEx meeting(s)
- SDT Subcommittee meetings to review applicable industry input on white paper

9. August 20–21 Meeting in Chicago, IL

- SDT Plenary and Subcommittee meetings to review and respond to industry input on white paper.

August 2009 — NERC Member Representative Committee, Presentation of the Phase 2 White Paper and Summary of Industry Comment and Response for MRC input, Winnipeg, Manitoba

10. September 9–10 Meeting in Denver, CO

- SDT Plenary review industry and MRC input on White paper and consider and agree on refinements
- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports
- Review Workplan through Summer, 2010, as needed

September WebEx meeting

- SDT Subcommittee drafting meetings

11. October 20–22 Meeting in New Orleans, LA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports
- Adopt Workplan through Summer, 2010, as needed

October WebEx meeting

- SDT Subcommittee drafting meetings

12. November 17–18 Meeting in Atlanta, GA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports

November WebEx meeting

- SDT Subcommittee drafting meetings

13. December 15–17 Meeting in Tampa, FL

- SDT Plenary Session(s)
- SDT Subcommittee drafting meetings

December WebEx meeting

- SDT Subcommittee meetings

Appendix #5 — Rep Markey's Letter to FERC

COMMITTEES
ENERGY AND COMMERCE
SUBCOMMITTEE ON ENERGY AND ENVIRONMENT
CHAIRMAN
SELECT COMMITTEE ON ENERGY INDEPENDENCE AND GLOBAL WARMING
CHAIRMAN
NATURAL RESOURCES

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836
DISTRICT OFFICES:
5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900
188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900
http://markey.house.gov

April 9, 2009

The Honorable Jon Wellinghoff
Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Dear Chairman Wellinghoff:

I have long been concerned about threats to our energy infrastructure, from terrorist attacks on LNG facilities to assaults on nuclear power plants from the air or the ground. Recent reports raise concerns about a more modern threat: cyber attack to our nation's electricity generation and transmission infrastructure. This matter warrants serious attention and I ask your assistance as we investigate the nature of the threat and what can be done to repel it.

As you know, the North American Electric Reliability Corporation, which is mandated to ensure the reliability of the nation's electricity supply, recently completed a survey of industry stakeholders to determine compliance with the Critical Cyber Asset Identification Standard. The results of this survey raise two issues of serious concern. First, the survey makes clear that industry has not fully adhered to this Standard, which is only concerned with identifying – not defending – facilities and equipment critical to the reliability of the electrical supply. This lack of adherence by industry to the Standard is disturbing because it indicates the vulnerability of the nation's electrical grid to cyber attack. If we have not yet even identified which assets need to be defended from cyber attack, how can we possibly defend them?

The second, and more disturbing, concern arises from recent news reports that the computer-based infrastructures of the grid have been repeatedly and systematically compromised through the Internet by foreign nations and groups. All Americans are troubled to learn that foreign nations and potentially hostile groups are apparently preparing a detailed "map" of the grid and its vulnerabilities, possibly to be used to facilitate some sort of attack in the future.

In light of these reports on growing threats to our electrical grid, I request additional information on what steps the Federal Energy Regulatory Commission (FERC) is taking to respond to these threats in the near term and prevent such breaches in the future.

In January of 2008, FERC approved eight mandatory critical infrastructure protection (CIP) standards, as developed by the North American Electric Reliability Corporation, to protect the nation's grid from cyber security attacks and other reliability breaches. The mandatory reliability standards required certain users, owners and operators of the bulk power system to

establish policies, plans and procedures to safeguard physical and electronic access to control systems, to train personnel on security matters, to report security incidents, and to be prepared to recover from a cyber incident. These standards were to provide a "comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks."

Please answer the following questions regarding FERC's actions in response to these threats and what additional measures may need to be taken by the industry, the Commission, and by Congress.

- What is the Commission's view of the results of the North American Electric Reliability Corporation survey? What percentage of Critical Cyber Assets have been identified? What is the significance of the information backbone of the electric grid being compromised? What immediate steps is the industry taking to stop these breaches?
- If foreign nations or hostile groups already have gathered detailed information to develop a "map" of the electricity grid, what actions can be taken now to prevent this information from being used to attack the grid?
- Have the CIP standards been fully implemented by industry? If not, why not?
- Are the current CIP standards sufficient to prevent cyber-security attacks and to respond to breaches? If not, what additional standards are needed?
- Has FERC developed metrics to measure the efficacy of the CIP standards? If so, what are these metrics? If not, why not?
- What processes are on-going at NERC to identify the need for new cyber-security standards?
- Is too much discretion given to industry participants in creating the cyber-security standards, since two-thirds of the group's members must support a standard before it is adopted or modified?
- What authorities does FERC possess to prevent and respond to cyber-security threats and breaches? Does FERC need additional authorities to protect the electricity grid from these threats?

Thank you for the attention to these matters. If you have any questions regarding this request, please contact Will Huntington of my staff at 202-225-2836.

Sincerely,

Edward J. Markey

Edward J. Markey
Chairman
Subcommittee on Energy and
The Environment

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #6
Phase 2 White Paper (April 5, 2009)

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706
4/14/2009

CATEGORIZING CYBER SYSTEMS: AN APPROACH BASED ON IMPACT ON BES RELIABILITY FUNCTIONS 31

EXECUTIVE SUMMARY 31

INTRODUCTION 32

BES RELIABILITY FUNCTIONS 34

IDENTIFICATION OF BES ASSETS 34

CATEGORIZATION OF BES ASSETS 37

THIRD PARTY OVERSIGHT OF BES ASSETS AND THEIR CATEGORIZATION 37

IDENTIFICATION OF CYBER SYSTEMS 38

CATEGORIZATION OF CYBER SYSTEMS 39

Cyber system interconnections 41

FINAL CATEGORIZATION OF CYBER SYSTEM BASED ON OVERALL IMPACT ON THE BES 42

EFFECT OF CYBER SYSTEMS CATEGORIZATION ON REQUIREMENTS 44

CONCLUSION 44

CATEGORIZING CYBER SYSTEMS: AN APPROACH BASED ON IMPACT ON BES RELIABILITY FUNCTIONS

EXECUTIVE SUMMARY

Intentionally left blank – to be redacted last

INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards aimed at preserving and enhancing the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. One must not forget the overarching mission of preserving and enhancing the reliability of this system, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability and operability of these assets.

CIP-002 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment." In reviewing the current CIP-002 version, the drafting team considered FERC's comments in its Order 706 approving the Cyber Security Standards and common perceptions and observations from various other commenters. In particular, the Standard Drafting Team considered these characteristics of the current CIP-002 approach which needed to be addressed beyond a first revision standard:

- A piecemeal approach
- Not protecting assets needing protection
- Allows "gaming" in the application of the requirements
- Uses an all or nothing approach
- Concentrates on loss of an asset and requires more explicit consideration of loss of integrity or misuse

This paper describes an approach based on the concepts of NERC's definition of Adequate Level of Reliability (ALR) and the characteristics of the BES described therein that will achieve this ALR, namely:

1. The System is controlled to stay within acceptable limits during normal conditions;
2. The System performs acceptably after credible Contingencies;
3. The System limits the impact and scope of instability and Cascading Outages when they occur;
4. The System's Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The System's integrity can be restored promptly if it is lost; and
6. The System 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

In particular, the approach relies on the identification of functions which are essential to achieving these characteristics and the BES assets which support these functions. These BES assets may be defined as facilities, equipment or systems performing functions to ensure that the BES achieves an Adequate Level of Reliability.

The methodology proposes to identify all cyber systems essential to the reliable operation of these BES assets: one must note that a cyber system can itself be a BES asset if it directly performs one or more of the identified functions.

Once BES assets and their cyber systems are identified, the methodology proposes a two pronged categorization which results, on one side, in a categorization of BES assets based on their impact on the reliability and operability of the BES, and on the other, a categorization of their associated cyber systems and their elements based on their impact on the BES assets they support. A rigorous merger of the two categorizations for any given cyber system results in a deterministically derived categorization of each cyber system based on its impact on the BES.

One must note that the scope of the CIP Cyber Security standards as defined during the SAR drafting team discussions exclude the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment and systems regulated by US and Canadian nuclear regulatory bodies, since they are regulated outside of NERC. Note that there may be facilities, equipment or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear regulatory organizations, and would therefore be regulated under these NERC CIP standards. It is also worth noting is that the CIP Cyber Security Standards do not include those assets associated with BES Planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will however be cases where these types of BES Planning and market function systems may be required to be protected under the CIP standards if they meet the protection requirements of the Cyber Security Standards (e.g. if they are within an Electronic Security Perimeter which is subject to the standards).

The concepts associated with an impact based approach to determining the criticality of certain facilities, equipment and systems are particularly well covered in the Draft Volume 1 of NERC's Security Guideline for the Electric Sector: Identifying Critical Assets. The development of this guidance document was in direct response to a directive by FERC in Order 706. An additional important concept in this approach is the inclusion of assets based on their functions in the operation of the BES. The group is currently engaged in Part 2 of the series, which addresses the identification of Critical Cyber systems.

The concepts and approach in this paper draw on elements of approaches already defined in several presentations by members of the Cyber Security Standards Drafting Team for Order 706 (CSSDTO706) to the drafting team. The approach on the identification and classification of BES assets also draws heavily on the work done by the NERC Risk

Assessment Working Group on the Draft Security Guideline for the Electric Sector: Identifying Critical Assets and current work being done by this group in the Identification of Critical Cyber Assets. The presentations by CSSDTO706 members to the group include the application of a FIPS199-like approach to classifying Cyber systems, NIST integration, a cyber systems based approach and discussions on Guiding Principles used for development, as well as comments and discussions by other members of the drafting team.

The overall approach includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact based methodology to categorize its BES assets and the associated cyber systems engaged in the process, and finally the deterministic derivation of an overall impact based categorization of the cyber elements, with the anticipated application of cyber security requirements commensurate with that categorization. This is in keeping with 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.

BES RELIABILITY FUNCTIONS

A pre-requisite to the start of the identification of BES assets which affect the reliability and the operability of the BES is the identification of functions which support the characteristics of ALR.

These include, at a minimum, support for:

1. Generation for the BES
2. Transmission for the BES
3. Voltage and voltage stability in the BES
4. Frequency and frequency stability in the BES
5. Protection of BES generation and transmission equipment from damage
6. Control and operation of BES assets
7. Wide-area situational awareness for real-time BES reliability and operability
8. Restoration of the BES

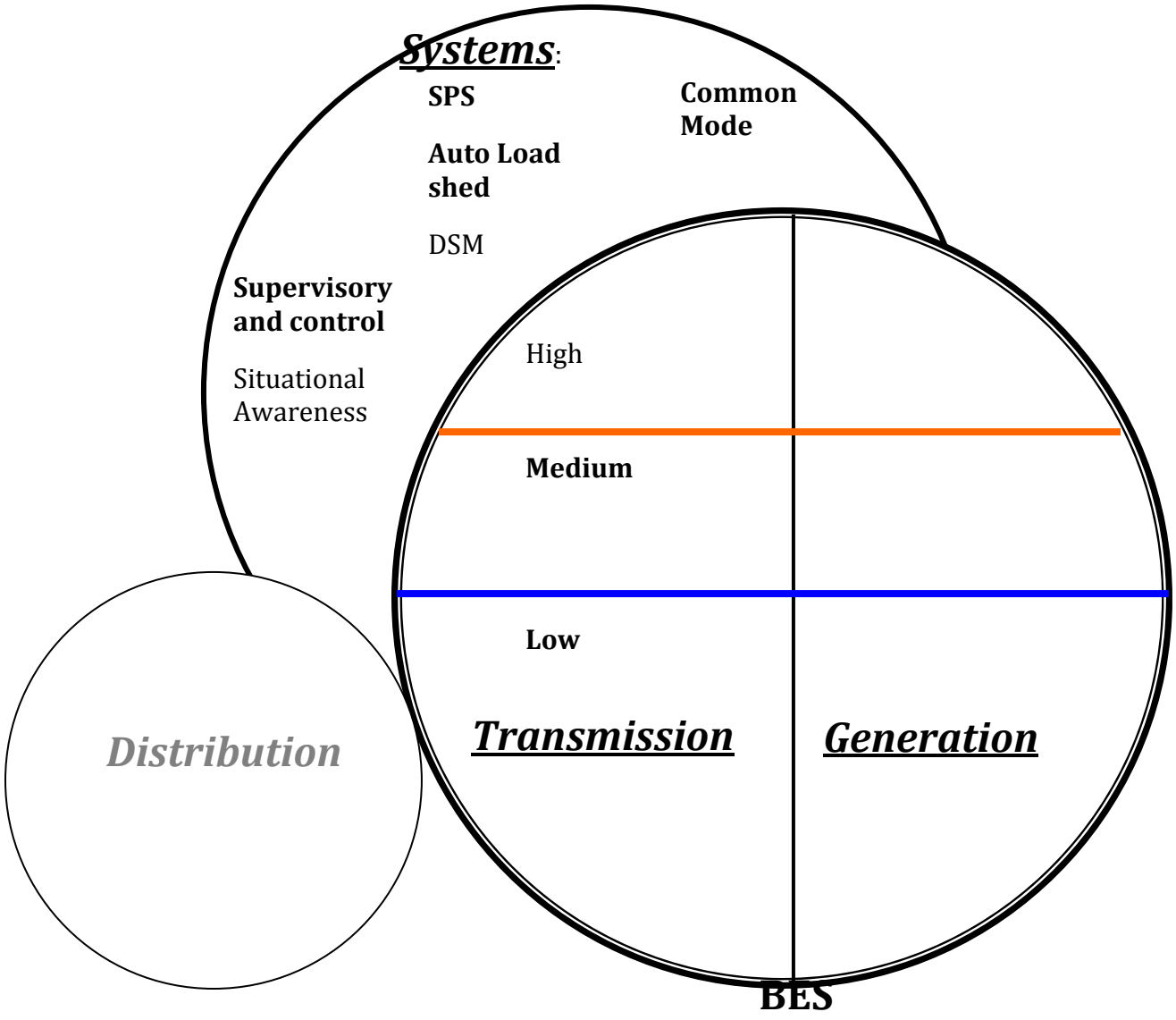
IDENTIFICATION OF BES ASSETS

The functions above are then used to identify all BES assets which support them. The inclusive list of these identified BES assets constitute the overall scope for application of criteria for their categorization based on their impact on the reliability and operability of the BES as defined by the characteristics of an ALR. In addition to facilities and equipment, the included BES assets must include systems which perform the following, at a minimum:

– Situational awareness

- Supervisory and control capability
- Special Protection Systems
- Systems essential to BES restoration
- Systems performing automatic load shedding
- Other systems that may perform a function directly related to the reliability or operability of the BES.

Bulk Power Assets



CATEGORIZATION OF BES ASSETS

(I would propose that we review the criteria defined in the Critical Asset Identification Guideline in the Transmission, Generation, Control Center and Special Systems sections (tables) be used as a minimum set for defining High Impact BES assets. I do not know how practical it is to ask a separate group, as discussed in the last SDT session, to come up with the categorization standards, unless substantial other work which can be translated into a categorization standard has already been done in this area. The guideline uses operating limits as credible criteria for determining criticality: I think the operating folks will be hard pressed further classifying this. Let's see what Dave Taylor provides at the next session. In the absence of adequate prior work, I am strongly tempted to propose using a 2 tier approach (i.e. a 2x3 matrix), High and Low for assets, and H,M,L for Cyber Systems. Anyway, whatever categorization scheme for assets goes here depending on what is determined).

Try for support from operations and planning committees to help define criteria for assigning assets to impact levels of high, medium, low, and none or others.

THIRD PARTY OVERSIGHT OF BES ASSETS AND THEIR CATEGORIZATION

An additional concept introduced in the approach is the inclusion of oversight of the critical asset list by entity types which have a more complete wide-area view of the BES. The approach uses a hierarchical approach to the oversight structure.

- Entities performing the functions of Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Transmission Operator, Generator Owner, Generator Operator, and/or Load Serving Entity submit their list of Critical Assets to their Reliability Coordinator for review.
- Each Reliability Coordinator submits its list of Critical Assets to its Regional Entity for review.
- Each Regional Entity submits its list of Critical Assets to NERC for review.
- NERC has its list of Critical Assets reviewed by the Regional Entities.

Based on their wider-area view, reviewers may add, but not remove, Critical Assets from lists and will provide justification for the addition of assets. In cases of disputes, there will be an arbitration process adjudicated by the next higher entity type.

The compliance responsibility of the identification and categorization of BES assets and their review and approval ultimately rests with the Responsible Entity owning and operating the assets.

IDENTIFICATION OF CYBER SYSTEMS

Two new terms have been introduced in this approach. The terms Cyber System and Cyber Component are defined in the glossary section of this paper. Cyber System is intended to replace the term Cyber Asset and more accurately represents the intended use of the term. Cyber Components are those discrete elements which make up the Cyber System (e.g. processors, disks, network interfaces, data). In particular, there have been some questions of whether requirements apply individually to the elements or the Cyber System as a whole. The use of these terms will hopefully clarify the intent of the application of these requirements.

Once the list(s) of BES assets have been defined, and all the essential functions performed by the BES Assets have been identified, the Responsible Entity uses this list to define those Cyber Systems which will support:

- The operation and control of these BES assets

  Examples of these are HMI systems in Generating Stations and Transmission Substations, Generating Plant DCS systems, RTUs and PLCs with control and operation functions for BES elements, EMS systems providing control and operate functions for operators *(review examples from CA Guideline)*

- The monitoring and alerting functions for the reliability and operability of these BES assets

  Examples of these are RTUs providing remote metering functions, Dynamic Feeder Rating systems *(review examples from CA Guideline)*

- The data acquisition equipment and systems which support wide-area situation awareness for automated or operator assisted real-time reliable operation of these BES assets

  Examples include Phasor Measurement Units when used in State Estimators for real-time operator assisted actions/alerts. *(review examples from CA Guideline)*

Any BES and non-BES cyber system which directly exchanges data with these cyber systems and elements will be identified for assessment. The judicious design and definition of electronic security perimeters and the application of access controls to these perimeters should be considered by entities to avoid the over-inclusion of cyber systems which do not affect the reliability or operability of the BES. Connectivity considerations will be discussed further in a separate section of this document.

CATEGORIZATION OF CYBER SYSTEMS

The proposed criteria for the classification of these cyber systems are based on the criticality of the function they provide on the BES asset: for each cyber system, an assessment is made on the effect of loss or compromise of the system on the availability, integrity and/or confidentiality of the BES asset it supports. The classification proposed is a 3-tier classification into High, Medium and Low.

(Should we insert here a matrix with A, I, C and H,M,L which would determine how to end up with the categorization of the cyber system based on this assessment? The meaning of what H, M, L in each of the 3 legs of Infosec should also be included. This would be intended to provide some rigor in categorization rather than simply leaving the criteria for the assessment to the entity). Consider the "high-water mark" approach from NIST to determine the impact characteristic of each element. See the FIPS 199 as a reference.

All cyber systems which meet the criteria defined in the Identification of Cyber Systems section above must be within a defined ESP. If there is no communication from inside the ESP to the outside, there is no access point to the ESP.

Cyber systems which perform the functions defined in the Identification of Cyber Systems section above on a set of more than one BES assets will be evaluated based on the impact of the common mode failure or compromise and may be classified a High, Medium or Low impact.

It should be noted that cyber systems which have a common mode impact on a set of BES assets and meet threshold criteria for affecting the reliability and operability of the BES should have been classified as BES assets, and these cyber systems will be assessed based on the common mode impact.

Systems classified as Critical Cyber Assets in versions 1 and 2 of CIP-002 (excepting those non-critical cyber assets that are in the same ESP) would be classified as high impact cyber systems.

Discussion of Cyber System Interconnections Impacts --– Phil

The proposed criterion for the classification of BES Cyber Systems is based on the impact to the function they provide or BES Asset they support: for each Cyber System, an organization determines the impact to the BES of the Cyber System's loss of confidentiality, integrity and availability. Categories of impact are defined as follows:

The potential impact is **High** if the loss of confidentiality, integrity, or availability directly causes or contributes to BES instability, separation, or a cascading sequence of failures, or places the BES at an unacceptable risk of instability, separation, or cascading failures.

The potential impact is **Medium** if the loss of confidentiality, integrity, or availability directly affects the electrical state or the capability of the BES, or the ability to effectively

monitor and control the Bulk-Power System, but is unlikely to lead to BES instability, separation, or cascading failures.

The potential impact is **Low** if the loss of confidentiality, integrity, or availability would not be expected to affect the electrical state or capability of the BES or the ability to effectively monitor and control the BES.

To perform the impact assessment, the organization would assign BES function types and/or BES Assets to each applicable Cyber System. Then for each function type and/or asset, the organization would determine the ~~BES~~ impact on the BES asset/s or function/s based on the loss of confidentiality, integrity, or availability within the Cyber System.

This methodology recognizes that a single Cyber System may support multiple BES function types and/or BES assets as shown in Figure 1. For example, a SCADA system may provide control functionality to a generator with minimal impact on the BES. However, the same SCADA system also provides control for substations on a high impact transmission line. So the organization would assign the final security categorization as *High* for the SCADA system.

This categorization approach makes two important advancements to ensuring a more complete and accurate assessment of Cyber System impact to the BES. First of all, the impact analysis requires a consideration of all BES functions and assets that the Cyber System provides or supports. Secondly, the final categorization ties directly to the security requirements of the Cyber System. As a result, the later security control selection should have its basis in reducing risk to the BES caused by a security breach in Cyber Systems.

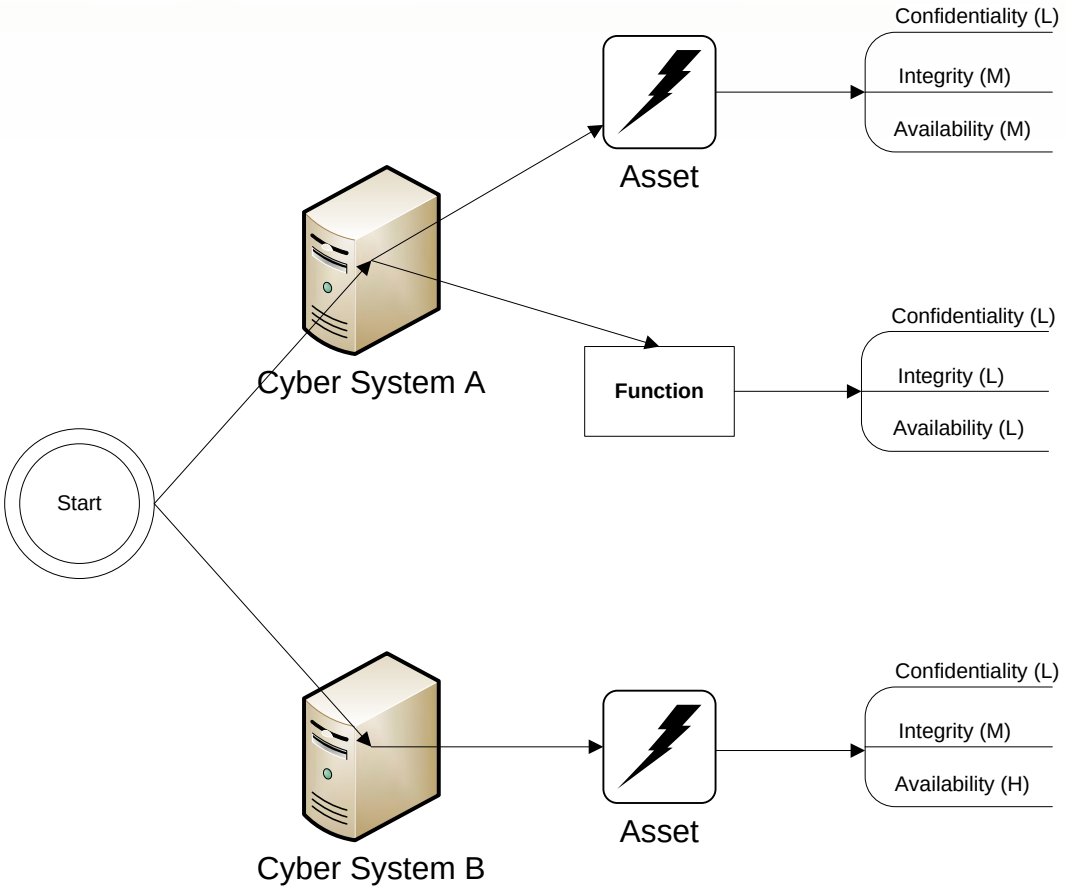


Figure 1: Cyber System Security Impact Analysis

Cyber system interconnections

Many BES Cyber Systems exist within a complex network of interconnected systems and exchange information necessary for the reliable operation of the BES. Just as downstream fault could cause cascading power outages, so a security breach in one Cyber System could utilize a trusted path to affect systems outside of an organization. Consequently, the security assurance of the Cyber System should reflect the level of risk associated with any interconnections.

Since this document only addresses the selection and impact analysis of BES Cyber Systems, the exercise of documenting and protecting interconnections is left as a security control to apply to the target Cyber Systems. However, the identification of essential interconnections into a Cyber System indirectly has a role in identifying BES Cyber Systems. For example, if Utility A classifies one of its Cyber Systems *High* and identifies an essential Cyber System interconnection with Utility B, then Utility B must consider the interconnected system in its BES impact categorization.

The drafting team recognizes the complex nature of interconnected systems and feels the Cyber System connection controls should be non-prescriptive. An organization should define, authorize and monitor connections as part of its secure operation of the Cyber System. An agreement should also be in place between two Responsible Entities to ensure the communication and consideration of Cyber System interconnections.

This approach ensures the standards address the complex nature of Cyber Systems operating the BES and assist organizations operating Cyber Systems downstream to understand the impact these systems have to the BES.

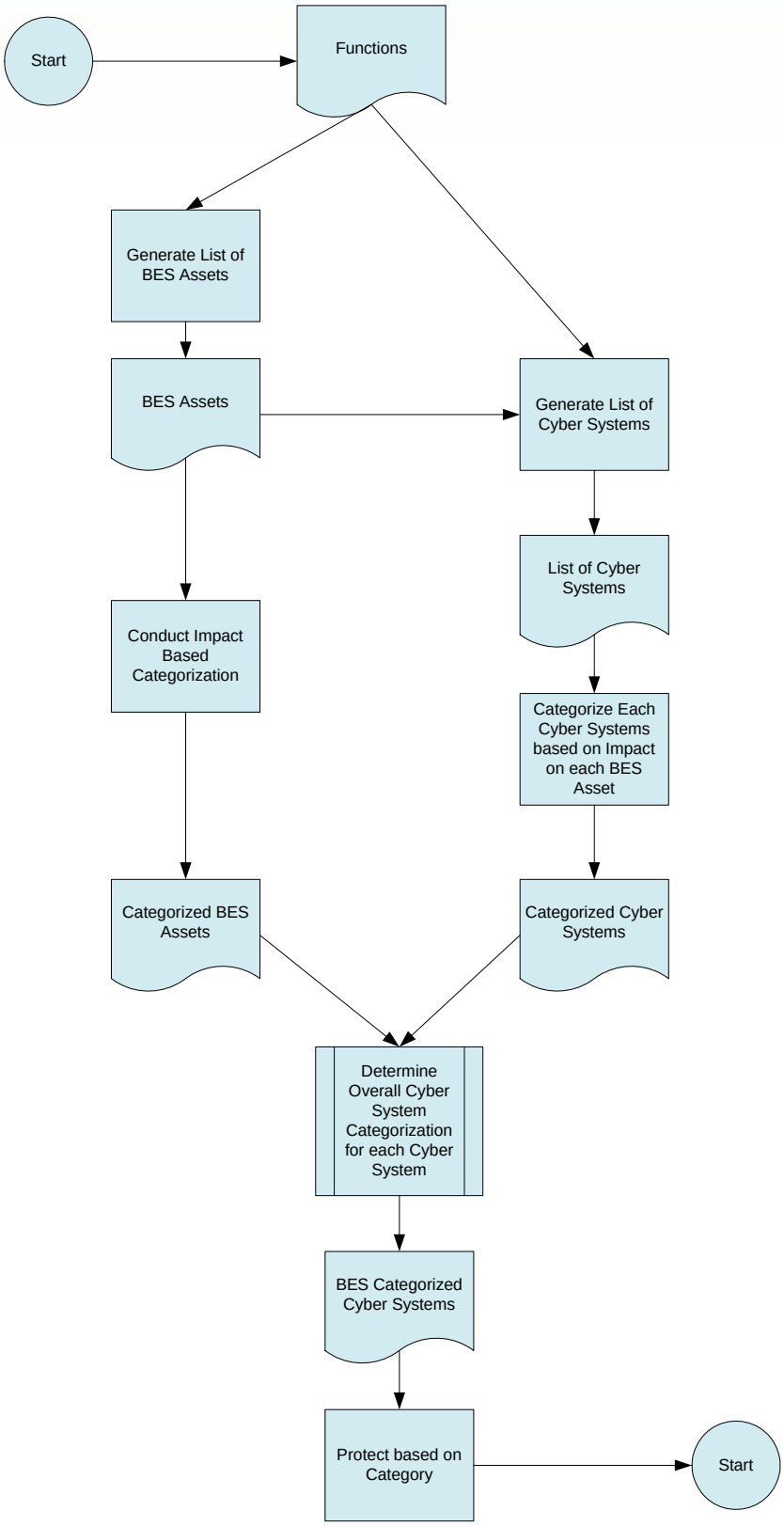
FINAL CATEGORIZATION OF CYBER SYSTEM BASED ON OVERALL IMPACT ON THE BES

The final categorization of each cyber system is determined by the application of a matrix which has predetermined outcomes based on the supported BES asset categorization and the categorization of the cyber system derived from its impact on the BES asset it supports.

This deterministic methodology will provide a more consistent approach than the looser requirement of any risk-based methodology in CIP-002-1 and CIP-002-2. The approach is based on an impact based methodology and will provide for more uniform application of a methodology for categorizing cyber systems.

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

Asset Impact -->	High	Medium	Low	None
Cyber Impact:				
High	5	4	3	1
Medium	4	3	2	1
Low	3	2	1	0
None	2	1	0	0


Start
Functions
Generate List of BES Assets
BES Assets
Generate List of Cyber Systems
List of Cyber Systems
Conduct Impact Based Categorization
Categorize Each Cyber Systems based on Impact on each BES Asset
Categorized BES Assets
Categorized Cyber Systems
Determine Overall Cyber System Categorization for each Cyber System
BES Categorized Cyber Systems
Protect based on Category
Start

EFFECT OF CYBER SYSTEMS CATEGORIZATION ON REQUIREMENTS

CIP-002 provides for the identification and categorization of BES cyber systems. Once categorized, the definition and applicability of requirements based on the category of the cyber system must be completed throughout the standards. This paper proposes that the current overall control (requirement) grouping in the respective CIP standard be kept wherever possible. The Drafting Team will review, change and augment the requirements in these standards as necessary and appropriate based on an analysis of the catalog of controls in the NIST guidelines when mapped to the CIP requirements. It must be noted that the High, Medium and Low categorization resulting from the proposed CIP approach does not necessarily correspond to the categorization levels defined in the NIST guidelines. This should be resolved during the analysis and mapping of the CIP requirements to the NIST controls by the Drafting Team.

In particular, in the review of these standards, this paper proposes that consideration be made for the different general cyber system types and their capabilities. In particular, the Drafting Team will consider differences in characteristics of cyber systems built on general-purpose platforms from proprietary purpose-built systems. The Drafting Team recognizes that proprietary purpose-built systems may have vulnerabilities similar to general-purpose systems. The Drafting Team will consider the preponderance of purpose-built systems and the implication on exception management, oversight and enforcement.

The Drafting Team will also consider the differences in transmission field and substation, generating plant and control center, equipment types and operating environments, and evaluate an approach to include them without unduly providing exceptions in the standards.

CONCLUSION

The approach proposed in this paper builds on work which the industry has already done in complying with the current standards, the guidance to be available soon in using a risk-based methodology for classifying BES assets, the industry's experience and investments in current compliance programs, and a recognition that the reliability of the BES is based on an engineered system increasingly supported by cyber systems. It is an incremental approach and addresses many areas of the perceived or real deficiencies in the current CIP-002 standard. It certainly ensures that all cyber systems related to the reliable operation of the BES are required to implement a security posture commensurate to the level of criticality of the BES assets they are supporting.

Action Items:

1. John — Will prepare the Introductory paragraph additions
2. Phil — Cyber Security Impact assessment description
3. Jackie — Categorization levels for impacts write-up
4. Scott — List of committees and disciplines for BES analysis support
5. Scott — John Sykes example white paper
6. ALL — send all inputs to John by Friday (4/3/09) for incorporation in to the next version.