NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

March 10, 2009 | 1–5 p.m. EST
March 11, 2009 | 8 a.m.–5 p.m. EST
March 12, 2009 | 8 a.m.–noon EST
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Meeting Summary Contents

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

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer, welcomed Frank Kim, Power System IT oversight — Ontario Hydro as a new member of the SDT replacing Michael Winters. She also noted that this meeting will be Tom Hoffsetter's last meeting on the SDT as he will be taking a position with NERC in their compliance group. She also noted that Bryan Singer had resigned as he is unable to fully participate in the SDT. Finally, Kevin Perry, Vice Chair, noted that he would be taking up a new position as SPP director of Critical Infrastructure Protection.

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.

NERC staff indicated the Technical Feasibility Exception white paper is being prepared for posting for industry comment. If posted promptly, the TFE posting will occur within the 14 day window the SDT agreed to when it approved the Phase 1 products for industry review, and thereby permit industry balloting of the Phase 1 products to begin in early April 2009. Regional entities received an early preview and briefing of the TFE white paper for any compliance and resource implications associated with the TFEs. Michael Assante, CSO at NERC, met with FERC staff to brief them on the TFE and the SDT 706 Phase 1 products.

Dave Taylor set out the process for developing the Version 2 Violation Security Levels (VSLs) noting that NERC was seeking to post the VSLs by Monday, March 16 in coordination with the Version 1 VSLs. He noted the plan is to pre-ballot review for Version 2 (that applies to the SDT's Phase I products) by May 11, 2009 and provide a 30-day industry comment period. On day-three, David Taylor reviewed with the SDT the Violation Risk Factors (VRFs) associated with the Cyber Security standards, and these were unanimously adopted by the SDT.

Joe Bucciero reviewed the Phase 1 Response document that was circulated to the Team earlier in March and the SDT unanimously adopted the response document for posting.

The facilitators reviewed the Phase 2 concept development which was initiated in the fall of 2008 by the SDT. In November there were criteria suggested for the design of the process. In December there were presentations and discussions regarding risk management. In January and

February 2009 two concept papers were developed that looked at two approaches to Phase 2: one which worked within the current CIP and sought to integrate applicable NIST and other ideas; the other started with a review of the NIST approach and sought to bring some of the CIP elements into a NIST-like model. At the conclusion of the February 18-19, 2009 meeting, the SDT asked the two teams working on the concepts to produce an initial draft of a CIP-002 standard that would be consistent with their concepts. These CIP-002 concept papers were reviewed, compared, and considered for possibly merger.

Bill Winters and Phil Huff presented a CIP-002 strawman alternative (Strawman A) developed by one team since the February meeting. The concept suggested:

- Assign 'functions' to systems
- Identify BES cyber systems
- Engineering studies used to develop Impact Criteria
- Use criteria in calculation of impact (integrity, availability, confidentiality)
- Categorization process (hi, med, low, none)
- Categorized BES cyber systems.

The discussion that followed covered issues such as: Connectivity to Networks; Increase in the scope of the CIP; Role of RROs and REs; Focus on information security; Updates for the standards; Boundaries; and 3rd Party Review.

Jackie Collett presented a second CIP-002 strawman (Strawman B). She noted that the CIPC Risk Assessment Working Group's (RAWG) work and draft report were helpful in the preparation and thinking for the concept paper. The CIP-002 concept paper started with the connections to BES-which is an engineered system. Cyber assets support the reliability of the BES. She suggested the strawman approach builds on: industry work, experience and investments in compliance programs but noted that the identified risks will increase scope of compliance. The concept paper addresses facilities, equipment, and systems, but acknowledges a need to better define systems going forward. The approach is not a risk assessment, but an impact assessment of the reliability of the BES. The CIPC RAWG work focuses on "impacts." Cyber assets are one of many elements supporting the BES processes. The concept paper proposes that properly applying a top down approach will ensure the reliability of the BES. She suggested the SDT should consider including some concepts from the RAWG in the new CIP-002 standard where it makes sense. The approach included in the strawman avoids being prescriptive but considers categorization of the BES assets as critical or not. The approach also considers the impact of the associated cyber assets as (3) low, (2) moderate, (1) high, and possibly none. The oversight of critical asset lists remains an open question at this point. The approach suggests using and incorporating NIST controls as a good starting point.

The discussion that followed covered issues such as: degree of flexibility and prescription; engineering-based assessment; list of cyber assets; and implementation phase.

As a follow-up to the discussion, the SDT members were given a brief survey to evaluate the two proposed approaches. The SDT reviewed the results of the overnight member survey, which suggested that the strawman approaches were generally in alignment with the overriding principles and have more in common than they differ. The facilitators asked members to offer elements of the strawman approaches they felt were strengths: (1) the simplicity and the definitions of Strawman A; (2) the critical asset identification associated with the BES that addresses the interrelationships of engineering, electric, and cyber systems in Strawman B.

The SDT discussed and refined the following common propositions drawn from day one's discussion on the two CIP-002 strawman approaches:

1. Existing CIP language is insufficient for the future
2. Ground the approach in the context of NERC's 6 elements of reliability adding cyber security to each
3. Utilize the graduated levels (high, moderate, low, and "who cares") in the approach
4. Include systems, facilities, and equipment *(build on the CIPC Working Group Draft Guidelines)*
5. Provide for 3rd party oversight and accountability in the process
6. Address the external interfaces impacting on BES reliability
7. Build upon existing controls such as the NIST 800-53 suite of controls

The facilitators suggested several discussion questions following the presentations and discussion of the strawman options including:

- What is the best place for the CIP-002 approach to start? From facilities? From Systems? From either? From both?
- What is the best approach to 3rd party oversight and accountability?
- What is the best approach to addressing external interfaces?

After some discussion, the SDT members agreed to break into two small discussion groups on the morning of Day Two to explore and focus on the possible merger of the two strawman approaches and concepts. Following lunch, each group reported the results of their discussion and engaged in a full SDT discussion of the issues.

The proposed structure of the draft CIP-002 standard has the following six requirements:

R1 — Identification of BES Assets
R2 — Critical Asset Identification Method
R3 — Critical Asset Identification

R4 — Cyber Asset Identification
R5 — Categorization of Cyber Assets
R6 — Annual Approval

The small group looking at Requirement R1 explored the possibility of merging a "facilities vs. functional" approach. They agreed that the starting point should be to identify the functions necessary for the reliability of the BES. The group agreed that it would then be necessary to identify the systems or hardware used to perform those functions. It would then be necessary to incorporate the high, moderate, low impact threshold each into category.

The small group looking at Requirement R4 suggested that the "systems" references should be taken out of R1 and only the "functions" of the BES should be included in R1. Requirement R4 should then identify the systems that support and perform the R1 functions.

Scott Mix presented a strawman for an approach to CIP-002 Requirements R2 and R3 for consideration by the SDT. He suggested starting with the functions and mapping them to the physical equipment. Consider determining "Asset Impact" as high, moderate, low, and none and "Cyber impact" as high, moderate, low, and none for CIP 003-009. After discussion the SDT ranked the three proposals:

Proposal 1 Keep R2 + R3 with Scott's Language (Matrix) (Average 2.9 of 4)
Proposal 2 Move R2 & R3 into R5 (Vector Analysis) (Average 2.7 of 4)
Proposal 3 R2 + R3 Performed by External Entity (Average 1.8 of 4)

The SDT agreed these proposals needed further review and consideration in the context of a single, coordinated approach.

At the end of the second day, a small group agreed to work further to draft a common framework. The group included Phil Huff, John Lim, Scott Mix, Jackie Collett, Scott Rosenberg and John Varnell. Jackie Collett introduced a flow chart as a strawman designed to be flexible to allow for further development and refinements, and it focuses on cyber systems (not on assets) and does not offer a hierarchal model. The "vector" categorization- matrix offers some more granularity as to what we are meaning to accomplish. It offers a cyber impact analysis of the impacts on the functions.

Following the discussion, the SDT agreed to rank the acceptability of the following proposition:

The SDT should adopt this approach as a working conceptual model to develop and frame a concept white paper that includes a set of definitions/glossary, develops a list of functions, and uses lists of scenarios to test the concept.

Acceptability	*4 =*	*3 = acceptable, I*	*2 = not acceptable unless*	*1 = not*	*Avg.*

Ranking Scale	*acceptable, I agree*	*agree with minor reservations*	*major reservations addressed*	*acceptable*	
3-12 SDT rank	**15**	**3** *(1/2)*	**1**	**1**	**3.6 of 4**
Second Rank with D Norton's Concept	**15**	**3**	**2**	**0**	**3.65 of 4**

During the discussion of the approach going forward, concern was expressed about whether the SDT was the right group to develop the concepts for Requirements 1,2, and 3 (the left hand side). Planning and operations perspectives would be helpful. Dave Taylor volunteered and the SDT agreed that he should draft a white paper to present to the next meeting on a process for determining Requirements 1, 2, and 3.

CIP-002 Common Framework Concept

Identification of BES functions which support the reliability and operability of the BES

Need 1 layer of specificity below ALR

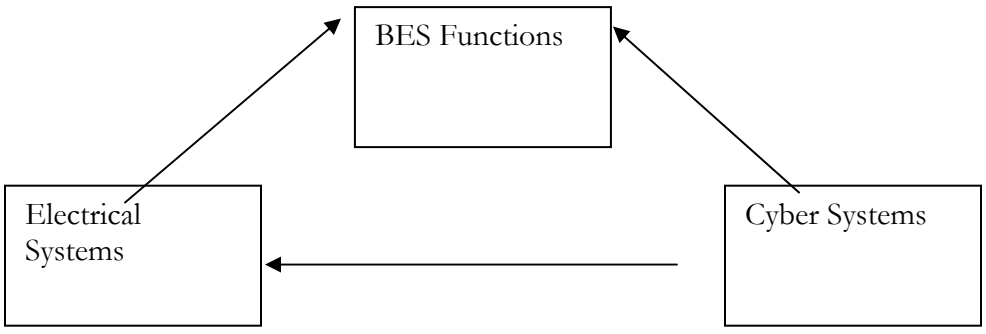
Cyber Impact — the local impact due to loss of CIA of the cyber asset for a BES element

System — a set of components which must work together

Electric System — a set of BES elements which must work together

Cyber System — a set of cyber components which must work together

Pre-Determined Functions			
R1	List of Electric Systems which support the BES functions	R4	List of Cyber Systems which support the Electric Systems and/or BES Functions
R2	Method of Categorization - impact to BES	R5	Method of Categorization - local impact to Electric System components
R3	List of Systems & Categories	R6	List of Systems & Categories
R7	Matrix: combines the 2 impact levels		
R8	Local Approval		
R9	Oversight		



Bill Winters requested the SDT rank the following proposition that if acceptable would be incorporated into the white paper going forward as the CIP-002 intent statement:

CIP-002 is intended to provide a discovery methodology that will lead to explicit identification and categorization of all cyber elements that perform or support BES functions. (3.9 of 4)

The SDT agreed that a helpful next step would be to refine the concept that was presented and tested on the third day to be in the form of a draft white paper. The chair asked Jackie Collett, John Lim, Bill Winters, and Phil Huff along with Scott Mix to take the lead in the development of the draft white paper in advance of the April meeting, building on the discussion and outcomes of this meeting. Other members would be welcome to send ideas and reactions as well as listen in and participate on the WebEx meetings that would be convened. The goal would be to share the white paper with the industry following either the May, 2009 or June, 2009 meeting.

The SDT members completed calendar forms regarding possible dates for future SDT meetings. Upon review of the forms and SDT member scheduling conflicts, the following dates and tentative locations were established and agreed to by the team.

Project 2008-06 — CSO 706 SDT
Proposed Dates and Locations for Future Meetings 2009

Dates in 2009	Location
April 14–16	Charlotte, NC
May 13–14	Boulder City, NV
June 17–18	Portland, OR
July 13–14	Toronto, CA
August 20–21	Chicago, IL
September 9–10	Denver, CO
October 20–22	New Orleans, LA
November 17–18	Atlanta, GA
December 15–17	Key West or FRCC (Tampa, FL)

The SDT agreed to seek to make a progress report to the MRC at its May meeting in Arlington, Virginia and provide a substantive briefing on the Phase 2 white paper for input at their August meeting. The team discussed the timing and objectives for a workshop. The SDT decided to hold open the question of convening an expert/stakeholder workshop pending the Chair and Vice Chair's discussion with Michael Assante, NERC Chief Security Officer, to gain a clearer understanding of the potential objectives, design, and timing of a workshop in light of the SDT's progress and schedule.

The facilitators offered some observations on the SDT's work over the past six months and suggested it would be timely to survey the team on the experience over the past six months to provide an opportunity for deeper shared reflections on the ways to improve the team's process.

The chair asked the facilitators to develop and distribute a survey to review the results at the April meeting.

The meeting adjourned at 11:30 a.m. on March 12, 2009.

I. Introductions, Agenda Review and Review of SDT Work plan

The Chair, Jeri Domingo-Brewer, welcomed the members. She welcomed Frank Kim, Power System IT oversight — Ontario Hydro as a new member of the SDT replacing Michael Winters. She also noted that this meeting will be Tom Hoffstetter's last meeting on the SDT as he will be starting work with NERC in their compliance group. She also noted that Bryan Singer had resigned as he was chairing a related group and had been unable to fully participate in the SDT. Finally, Kevin Perry, Vice Chair, noted that he would be taking up a new position as SPP director of Critical Infrastructure Protection.

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.

Mr. Bucciero reviewed with the team the need to comply with NERC's Antitrust Guidelines. He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. 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 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. (*See Appendix #4)*

II. Technical Feasibility Exception Update and SDT Discussion

Scott Mix noted that NERC staff believes it is ready for posting for industry comment. Regional entities will receive an early preview of the TFE for any compliance and resource implications (March 6). Michael Assante, CSO at NERC met with FERC staff to brief them on the TFE and the SDT 706 Phase 1. He noted that Dave Cook, NERC General Counsel indicated that the target was to post the TFE at end of week. This would bring it within the 14 days the SDT agreed to when it approved the phase 1 products for industry review. This would allow industry balloting starting in early April.

SDT Member comments

- Any substantial change since December? As was discussed in the February 18-19 SDT meeting, the TFE can be claimed only where it is specifically allowed to be claimed under the FERC Order 706.
- SDT may support a TFE through a standard modification regarding operations and safety in phase II.

- Removing risk acceptance- didn't put back in where "technically feasible" requirement for compensating measures. Just not a procedure through the TFE. Like documenting the compensating controls.
- The SDT can deal with TFE in Phase 2 standards
- People in industry are worried- when will they get it? TFE not applicable to every standard and requirement.
- R5- would language have to exist in each sub-requirement? No, if in main requirement applies to all sub-requirements.
- Applicability model will be part of the posting for TFE? Yes it is there.

III. VSL and VSR Committee Update

Dave Taylor set out the process for developing the Version 2 VSLs. He noted that NERC was seeking to get the Version 1 VSL document posted by Monday, March 16. He noted the plan is to pre-ballot review for Version 2 VSL (i.e. Phase 1) by May 11, 2009 and provide a 30 day industry comment period.

SDT Member Comments on VSLs

- Interrelationship between the two VSLs need to be clarified for the industry.
- If industry doesn't approve version 2 (i.e. Phase I) CIPs OR the VSLs, NERC will have to file something with FERC. The NERC BOT has to approve any filing. May take a BOT override on the process.
- Along with VSL and standards timing. Industry needs to understand the TFE process. Many things to understand in terms of the inter-relationships.
- NERC planning to launch a separate web page and a separate announcement and a note in the NERC newsletter.
- NERC should consider making a "Gant chart" on web page- highlighting the timing for review and adoption with definitions of what they each do and why it is important that they happen in the right timing.
- Is NERC planning on providing information to the ballot body of the ramifications of a failed Phase I ballot? Industry should know what will happen if it fails to pass. Prefer to know beforehand what will happen.
- NERC needs to be careful about the perception of threatening the industry. NERC will do the bare minimum to meet FERC directive if the ballot doesn't pass.
- Can FERC be approached for an extension? No, it has already passed and it is now federal law.
- We need some kind of dialogue mechanism with the industry- blog, webinar, get information to the industry. Need to careful about managing expectations about the turnaround.
- Who would be responding to industry questions? With what authority? etc. NERC would have to dedicate a full time person to response.

- What happens if registered ballot body votes down version 2 standards. This is a non-trivial thing in the era of the ERO. "Smoldering anomaly." Ask FERC- what do we can/should do. We played the game and industry won't budge. There is precedent for BOT overruling a no vote in the period before the current ERO status. In the era of ERO will this fly?
- Same problem with FAC standards-. NERC understands and has to follow the ANSI process.
- The audit issue in July may pose a unique problem and NERC might be able to get through the filing process without raising too many eyebrows.
- If Phase I does fail, NERC and the SDT should look at responses before make decisions what to take to FERC.
- We should encourage NERC all with ideas for engagement with the industry stressing the importance of a consistent message- Will NERC be going to all regions?
- SDT 706 Slide presentation to timelines- send to all members- Scott Mix- Dave Taylor , Joe Bucciero and Kelly at NERC will do so. Also work with regions through the team.

On day-three, David Taylor reviewed with the SDT the VRFs and additional language for Requirement 1.8, noting that most reviews were judge to be "medium". He asked for feedback on the proposed levels. He noted that if the SDT approved they would be posted today along with the Version 1 VSLs. A motion for the SDT to accept the draft (John Lim, Bill Winters 2nd) and unanimously adopted by the SDT (18-0).

IV. Phase I Response and Timeline

Joe Bucciero noted that the Phase 1 Response document was circulated to the team earlier in March for their review. The chair entertained a motion (Freese, Edwards 2nd) and the SDT unanimously approved the response document for posting.

V. Phase II Concept Development

Stu Langton noted that the Phase 2 concept development was initiated in the fall of 2008 by the SDT. In November there were criteria suggested for the design of the process. In December there were presentations and discussions regarding risk management. In January and February two concept papers were developed that looking at two approaches to Phase 2: one which worked within the current CIP and sought to integrate applicable NIST and other ideas; the other which started with a review of the NIST approach and sought to bring some of the CIP elements into a NIST-like model. At the conclusion of the February 18–19 meeting the SDT agreed to ask the two teams working on the concepts to produce an initial draft of CIP-002 consistent with their concepts for review and comparison and possibly merger.

A. CIP 002 Strawman #A — Concept Proposal Presentation Overview

Bill Winters presented the drafting team's CIP-002 strawman (See Appendix # 6) as was agreed at the February 18–19 SDT meeting. SDT members participating on the team included: Jerry Domingo Brewer, Phil Huff, Kevin Perry, John Southern, Keith Stoffer and Bill Winters. He noted they used Kevin Perry's concept paper presented at the last meeting as the guide for

developing the CIP 002 and that this was a systems-based approach in terms of systems control and systems awareness which started with looking at core function systems/assets. He described a reverse "peeling of the onion" approach, starting from the insider out. The team started with a series of "nested" definitions of cyber asset, cyber system and control systems- all nested within cyber systems.

The team's intent was to try to simplify a systems approach — e.g. start at your SCADA server, what is connected to it providing data to it, continuing to walk out to your historically system and on to determine full scope of the system using in control and system awareness. They sought to define one or more security boundaries (R2) then identity security boundaries around systems. They introduce a categorization criteria model (low, med high) to apply to cyber systems (R4.) That would be approved and reviewed at regional level. The approach allows some flexibility, region-to-region. E.g. working groups within regional entities could work to define for each region. Then remaining CIP standards apply. Deal with mapping to low, medium and high. (R5) Implement a change- need to assess. How to capture interconnected external entities (R7)

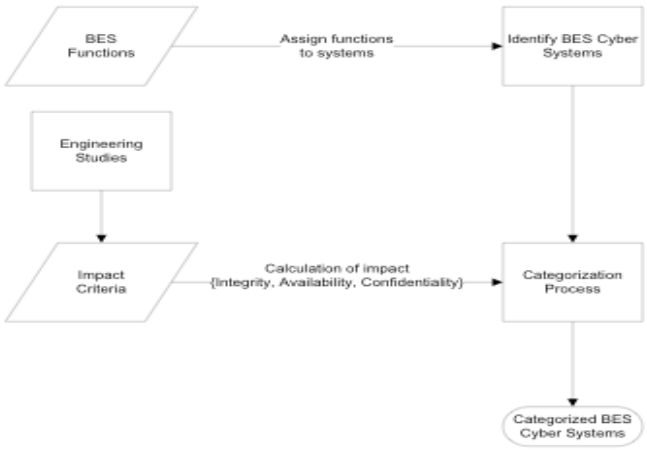
SDT Member Q & A and Discussion

- **Categorization at the regional level.** R4 — regional categorization? Which entity? The region itself. E.g. ERCOT. Do they have the capacity to do this? Regions will need to understand this approach going forward.
- Region would approve the criteria for the thresholds, e.g. less than 300 mw low, 300-800 moderate, above 800 high. Region wouldn't look at the cyber asset or system.
- **Confidentiality —** Are there confidentiality issues that need to be addressed with the approach? Establishing a framework for the categorization model- would be a risk impact model at a regional level.
- **Inconsistent regional interpretations —** If we regionalize decision making around R4- how does NERC deal with inconsistent interpretations?
- Regions might petition to NERC.
- Does R7 create a legal duty to do something? Why there? Concern we may have inconsistent responses across the regions, one entity take action against another?
- High medium and low- needs to be consistent across all regions and entities. What is in the standard is what is audited to. Sounds like a "fill in the blank" standard.
- **Connectivity to Networks —** Concern about idea of connectivity or network connectivity having been lost? Implies this evaluation of systems would have to take place on any equipment regardless of their connectivity to networks. Would all these have to be evaluated?
- Network communications was left out of the description because communications standards would take care of this. Systems approach looks at interconnection. Isolated item would be assessed for connectivity- unless it was in the "lower than low" category.
- Approach focuses on system and data exchanged within system and between systems.

- **Increase in scope —** A facility with serial connected devices collecting data would not be covered by the current CIP? This may pose a significant scope increase in terms of assessment.
- Terminology needs to be tightened. Ran into that in trying to implement and audit the current CIP standards. Need to make immediately obvious to anyone what is a reasonable understanding of what it is we are after in these standards.
- **RROs and REs —** Regional approval? Region doesn't exist- either RRO or RE. Is it a jurisdictional entity that requirements can be tied to? Regions RROs RE may not have technical competency to do this yet.
- **Focus on information security —** Are we focusing on hardware vs. information/data we need to perform functions that will come through different systems that are "data feeds?" Information security is the focus. Region is not where it is at. Reliability coordinators will need to decide this. Not operating in a vacuum. Region could have function of holding meetings of RCs.
- Look at the mission then look at the equipment. Different levels of requirement based on your threat profiles.
- There is a disconnect on how regions will apply this. One company can cover 5 regions. How will one system be treated with 5 regions telling us what to do. Needs to be applied the same. This is important and not sure how it will be taken care of in the "systems" approach.
- Jeri Domingo Brewer shared a presentation of how BOR does asset categorization process at the February 2-4 meeting in Phoenix. The same situation happened in the Federal sectors when they had to categorize their systems. There is a corporate impact that needs to be assessed if you lose functional capability.
- Address realities in how infrastructure is operated so that standards can be audited in a consistent manner.
- The SDT may be caught in the language. Focus instead on the approach that is being proposed. Fundamental to the approach is the way of arriving at which assets should be protected. IT marries a functional view with the traditional engineering approach. There will be follow on activities as to what to do with the standards.
- ERCOT region/ISO wide area visibility- criticality of any assets. ISO functioning as a RC? Lots of things to look at. If you declare assets to be critical that the responsible entity doesn't agree. Number of aspects are complicated need to recognize this.
- Acknowledge the point about addressing companies who straddle multiple regions. Didn't want NERC to mandate across the board what the threshold criteria would be. E.g. the nature of congestion of northeast may be different than that of the midwest etc.
- Engineering model applied to cyber asset vs. the other way around.
- **Updates —** Updating once every 3 years vs. annually. Consider all the assets that manage the grid. High moderate low and maybe "lower than low." After initial investment in the classification, the future efforts will be building on that.

- **Boundaries** — R2 — one or more boundaries allows flexibility. In concept paper did not represent telecommunications functioning- you can't manage or control it. Preserved the concept of it being out of scope-not including devices.
- Limit to Cyber systems that do something. Protect the data. Depending on where you draw your boundaries, scope of telecommunications.
- R7- doesn't exist in the standards today. Finds this to be a huge problem. Need to find a way to address. Calls for communication with external RE.
- **Critical** — The strawman doesn't use word critical. Current reliability standards — BPS — violation of risk factors high, medium low. Equivalency? Somebody has to protect anything that could possibly violate a requirement. Label that as a critical asset. If you violated that requirement because of cyber security incident.
- Look at existing tools and concepts used to try to determine how important things are.
- **3rd Party Review** — FERC order- appropriate 3rd party approval — region was an attempt. "appropriate 3rd party review to be determined"
- Description of the process proposed:
    - R1- scope your systems affecting BES. (kick out such things as customer service etc).
    - R4 Assess as low, medium, high.
    - Start with information — captures intent of CIP. 3rd party concept allows for not a solution but a requirement.
    - R3 prevent gaming.
    - R6 internal controls
    - R7- heartburn- negotiation and arbitration method to agree on a list- walk away equally unhappy.
    - "Networks" captured in cyber assets definition.
    - Better model for defining function.
    - Take approach for determining critical functions.
    - Public concern is with remote configuration capability (a la Aurora) engineering support and maintenance. Systems in place but with remote access.
    - Treatment — "my identify" password synchronization- HR system. Shut off access in a keystroke in Corporate IT land. What is a peripheral system?

On the afternoon of day two the following flowchart was presented and discussed:



Bill Winters presented the straw man A CIP-002 flow chart process and summarized the steps:

- Assign function to systems
- Identify BES cyber systems
- Engineering studies leading to Impact criteria
- Use criteria in Calculation of impact (integrity, available confidentiality)
- Categorization process (hi, med low, not)
- Categorized BES cyber systems.

SDT Member Comments on Strawman A Flowchart

- Incorporate engineering into categorization?
- Power systems and computer systems networks. 2 and 3 are power systems.
- Where do lists of functional impacts come from and at what point? (identify BES cyber systems)
- Shrink to cyber systems? Need to have all the pieces to perform a function? Shrink or whittled?
- Categorization to each cyber system on list- box? Oval- CIP standards on 002 applied to categorized BES cyber systems.

B. CIP-002 Strawman #B — Concept Proposal Presentation Overview — Jackie Collett, John Lim, Scott Rosenberg and John Varnell

Jackie Collett presented the team's CIP-002 strawman (*See Appendix #7).* She noted the ~~CIPSE~~CIPCCIPC Risk Assessment Working Group's (RAWG) work and draft report was helpful. Their concept started with the connection to BES — which is an engineered system. Cyber assets support the reliability of the BES. They address facilities, equipment and systems but acknowledge a need to define systems going forward. Their approach is not a risk but an impact assessment of the reliability of the BES. ~~CIPSE~~CIPCCIPC RAWG, focuses on "impacts." Cyber assets are one of many elements supporting the process. They propose that properly applying top down approach will ensure the reliability of the BES. She suggested the SDT should consider including some concepts from the RAWG in the standard where it makes sense. Their approach avoids a prescriptive approach but considers categorization of critical assets of BES — critical or not. Consider critical cyber assets: (3) low, (2) moderate, and (1) high and some that need no protection in transmission and generation. The oversight of critical asset lists- remains an open question at this point. Use and incorporate NIST controls that provide some good starting points.

She suggested the approach builds on: industry work, experience and investments in compliance programs but noted that the identified risks will increase scope of compliance. She then reviewed CIP 002 draft requirements and changes.

SDT Q & A Member Comments

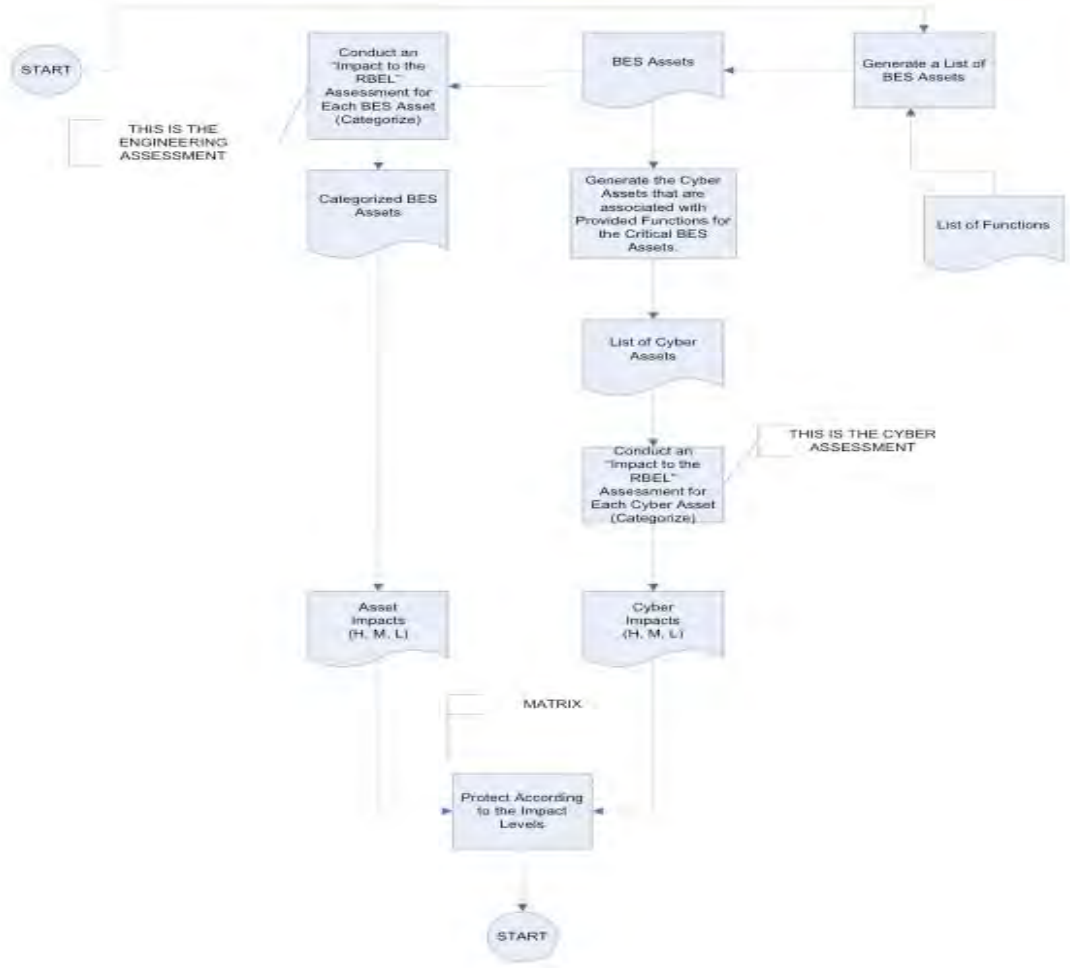
- What is the right balance between overly prescriptive and too loose?
- The six NEC principles of adequate levels of reliability can be core principles for developing standards. This will go a long way towards providing credibility for the SDT's proposed CIP standards.
- Didn't see a requirement for assessing the impact of the assets before assessing impact of cyber assets. This is a two-step process. Assess high, medium low none, on electrical assets

and then on cyber asset. Matrix: rigor for requirements. High and high highest level of rigor etc.

- Lends itself to NIST approach. Goes a long way
- The team agrees with these comments and left it out for simplicity case.
- The two strawman proposals (A & B) are not at polar opposites of positions. There are many commonalties with the main differences being the risk assessment vs. impact assessment.
- High impact? Critical asset that is also a cyber asset — current CIP don't address.
- EMS data system- cyber asset. Our control system (function) was the critical asset.
- Agree that there is a huge amount of judgment around identifying the assets.
- Why haven't we asked industry — to submit examples of excellent methodologies of categorizing assets? Did ask through the ~~CIPSE~~CIPCCIPC last year.
- Many are paid for methodologies and there is a reluctance to share methodologies based on issues of confidentiality.
- Cyber being a critical asset. Last drafting team- moved to function.
- Impact categorization- high medium low. Network automation-
- Substation lab with metering doesn't work through fire walls. Look at function of relay- may have some pieces not as important as others.
- Network automation "support" vs. "intrinsic" to the operation?
- How do we do this.
- A9- how far apart are we? End result of both approaches is a list of cyber assets. Both identify all. If critical assets — start with systems. Apply engineering criteria.
- Not all things considered as part of system. One looks first at physical then others supporting it.
- Both looking at impact of cyber system on reliability of the BES.
- Not just focusing on physical assets. Important to look at function. Inclusion of systems if they are assets related to that function.
- Strawman A suggests that threshold criteria for impact determination be set. Can we link criteria to adequate level of criteria?
- Difference from engineering look and then the other way around.
- Engineering based assessment is critical to both approaches. R4 — assess the risk of those systems. First criteria — what asset it supports 25 mw or 1000.
- Start with a list of systems or a list of assets. Starting point is the difference.
- Differences- one is bottom up and the other top down. Subtle differences in terminology. Asset vs. system.
- Consistent guidance in body of standards — white paper as an attachment to body of standard. De facto implementation guide. Consistent method of categorizing assets. Because it is part of standard, it becomes binding.
- E.g. operational standards — calculate ACE — formula is not in a requirement, but an attachment to a standard.

- It is during the implementation phase that we see big difference between approaches. If just securing systems, or facilities- limit the locale where we control access to computer rooms. Think if intent is to secure- both facilities and systems.
- Load study analysis as part of identifying critical asset list.
- 706 "guidelines"- white paper might serve as that? How to do things is a guideline. Do we write the guideline as a part of it? Who would do this? Not NERC staff. May need the standards, the implementation convention, guideline that talks about approaches. E.g. an attachment about what a high impact is.
- Prescriptive vs. non-prescriptive.
- Look at some existing standards- allowable method.
- Took "supporting functions" intent out of CIP 002 to not raise this? Can't audit an intent- intent can be in a white paper. Nature of guidelines — options

On the afternoon of day two the following flowchart was presented and discussed:



Jackie Collett presented a flow chart depicting their approach that included reference to Scott Mix's matrix.

SDT Member comments on the Strawman B 002 Flow Chart

- What is a cyber impact? Impact on the BES? Yes. Independent of impact on physical asset that it is controlling.
- Why bother generating list of cyber assets for low impact? Low represents some level of protection.
- The impact on that asset and impact on BES comes in through the use of the Mix matrix.

C. Strawman Proposals Alignment with Guiding Principles

At the end of the day the members agreed to complete a matrix that highlighted the degree of alignment of each strawman with the guiding principles developed by the SDT at its last meeting. The results were compiled overnight and were presented to launch the discussion on the second day.

The members suggested that the rankings supported the suggestion that the strawman approaches were generally in alignment with the principles and have more in common with each other.

SDT GUIDING PRINCIPLES	Strawman B – CIP-002 Lim et al.						Strawman A: CIP 002 Huff et al					
Alignment=	*Fully*	*Generally*	*Somewhat*	*Not*	*NA*	*Avg.*	*Fully*	*Generally*	*Somewhat*	*Not*	*NA*	*Avg.*
	4	*3*	*2*	*1*	*NA*	*Avg.*	*4*	*3*	*2*	*1*	*NA*	*Avg.*
1. Map CIPs to NIST 800-53 to help quantify and assess any gaps	**4**	**4**	**4**	**0**	**5**	**3.0**	**3**	**6**	**3**	**0**	**5**	**3.0**
2. Protection of communication devices outside the electronic security perimeters is out of scope.	**7**	**6**	**2**	**0**	**2**	**3.3**	**4**	**4**	**4**	**0**	**2**	**3.3**
3. Create non-prescriptive standards and employ a technical exception/ compensating measures documentation and guidance process to accommodate variations.	**2**	**9**	**0**	**0**	**3**	**3.2**	**0**	**8**	**6**	**0**	**3**	**2.6**
4. Strive to preserve existing security investments and build upon the existing CIP requirements.	**6**	**10**	**0**	**0**	**2**	**3.4**	**2**	**9**	**5**	**0**	**2**	**2.8**
5. Protect the integrity of data throughout its transit.	**4**	**4**	**5**	**1**	**3**	**2.8**	**4**	**5**	**4**	**1**	**3**	**2.9**
6. Consider the unique locational characteristics (e.g. substations, data centers, generation plant) and functional capabilities of the cyber assets to be protected in CIP requirements.	**4**	**8**	**0**	**0**	**0**	**3.3**	**7**	**6**	**3**	**1**	**0**	**3.1**
7. Use a consistent risk-based model to classify cyber assets (as critical/high impact, moderate impact, low impact) allowing for expansion of standards beyond "critical."	**7**	**7**	**2**	**1**	**0**	**3.2**	**7**	**6**	**3**	**1**	**0**	**3.1**
8. Consider the minimum security controls for high, moderate, low within NIST 800-53 to help model the CIP requirements for each level.	**6**	**6**	**1**	**1**	**3**	**3.2**	**4**	**7**	**3**	**0**	**3**	**3.1**

NOTE: The SDT acknowledges that currently an entity's cyber asset classification is subject to scrutiny by the compliance enforcement authority and applicable regulators. *(February 18, 2009)*

3–10 SDT Members Written Comments on Matrix Form:

- I like the Grid-based approach in principles 1-4. I believe the systems-based approach is the favored approach. I think the issue of starting point is key- i.e. what is it we are trying to protect.
- Principle #1- NIST is system-focused against mission, no asset based

- Principle #4 Both approaches end in a list of cyber assets

D. Strawman A & B Areas of Strengths and Commonalities

The facilitators asked members to offer elements of the strawman approaches they felt were strengths:

- Several liked critical asset identification of the Strawman B paper. Engineering. Electric and cyber system interrelated.
- Strawman B's identification of cyber assets touching BES. Deals with cherry picking today with cyber assets
- Strawman A's simplicity and definitions.

The facilitators offered the following straw common propositions drawn from day one's discussion on the two CIP 002 strawman approaches for the SDT's review and discussion:

1. The current CIP language is insufficient for the future.

~~1. The current CIP approach is not a sound basis going forward to protect cyber assets and BES reliability (as exhibited by the five issues identified by Jackie et al).~~

SDT Member comments and suggestions.

- Both groups agree but this statement is too negative
- We have a sound basis- need to improve upon. Started from ground zero. It was a starting point. Need to do better.
- Delete and substitute: "The current CIP language is insufficient for the future. "
- What is the starting point of the security standard? Focus on systems or facilities and systems?
- Do we need a different approach?
- Yes because the problem with current approach is inconsistent and non-uniform protection of cyber assets. Giving each responsible entity authority to devise various processes with no approval and oversight get to the crux of problem. Goal of standard should be to keep the lights on and protect the BES, not to maximize shareholder concern.
- Focus on closing the loop holes. Don't cut unnecessarily into innovation and flexibility.
- Have to look at and find agreement on the problems we are trying to solve so we can look at each option's ability to solve problems.

2. Ground the approach in the context of NERC's 6 elements of reliability adding cyber security to each.

SDT Member comments and suggestions

- This is not in Kevin's approach. Not documented.

- Probably need to add, “adding cyber security to each” at end of the statement.
- Protecting from cyber security attack might be the 7th element of reliability. Malicious compromise of an asset. Currently talk of “critical”- reliable enough to sustain a cyber attack. Thus need to address all electronic control devices- high medium low as to how
- Problem is not cyber attacks but configuration management.
- Knowledge of IT and info security is not widespread. Let’s ground this in problems we are facing.
- Who has a good inventory of what we each have and don’t have? Do we know what we are managing? Put emphasis here on “care and feeding”
- “Adequate level of reliability document”- cyber security not a 7th element of reliability. Adjunct to all other six elements. Cyber security so that… we can recover from contingency, etc.
- N-1 is a concept that can’t work in cyber security. What do you have to do for resiliency in the cyber world: confidentiality, integrity, availability. Probably not a 7th element.
- Address what is the minimum for reliable operations.
- Keep the goal in mind in terms of cyber- ensure reliable power withstand an attack. Believes should be a 7th element.
- “Support” – cyber security/ computing systems are integral. Primary critical- can’t run what we are doing without computers. Central to our thinking about the problem.
- What is the goal of standards? Mitigate the risk or deal with reliability in wake or presence of attack? Goal is to prevent, deflect or recover from the attack.
- Engineering vs. IT approaches. This was faced when the federal entities began dealing with NIST in 1998. They were mandated to protect both physical and cyber, interconnected network systems connected to physical infrastructures. Take digital world into account new threats grounded in engineering foundation. It takes both- CIO, engineering and CEO viewpoints to do the job and solve the problem.
- Smart grid discussions have identified 16 critical infrastructures
- What are we trying to protect? Where to focus our attention? On terror or hackers?
- Focus on impact to organization and assets/people mission when any of the triad is compromised. Don’t have good info on who we are trying to protect against. Get away from the vector causing the impact, focus instead on what to do to protect against impacts.
- Creating false divisions- IT won’t be doing the engineers’ jobs designing power system elements. Engineers need to understand IT principles.

- CIPS have done a good job opening eyes to engineers- they now appreciate IT security components. Build upon this—the CIPs that are good but need to get better. Even below 100KV is automating.
- CIP 002 is about classification- regardless of IT or engineering. Extend to IT systems or networks?
- Holistic approach to IT- many threats from inside network. Not focusing on who but on what and where.
- CIP has both engineering and IT portions. 3 layers of classification will be helpful to them. CIP 002 needs to do both. More of an engineering function.

3. Utilize the ~~NIST~~ graduated levels (high, moderate low, and "who cares") in the approach.
   SDT Member comments and suggestions
   - Is this in terms of controls?
   - We have lost FIPS 199 in that. Self-assessment of impact to mission.
   - Assessment of impact to mission.
   - JP: value of exploring categorization of critical assets. Covered in concept paper. Impact assessment- organizational or asset?
   - Need to add a "inconsequential" or "who cares" level, lower than low.
   - How many levels we need? 3 right approach. FIPS 199 is using 4.

4. Include systems, facilities and equipment *(build on the ~~CIPSE~~CIPCCIPC Working Group Draft Guidelines)*
   SDT Member comments and suggestions
   - Everyone needs to look at guideline before we can agree to "build on".
   - Focused on identifying critical assets- CIP 2 version 1. Would have to modify it for both approaches.

5. Provide for 3rd party oversight and accountability in approach

6. Address the external interfaces impacting on BES reliability
   SDT Member comments and suggestions
   - Is this addressed in Strawman A only? Strawman B team agrees with this and do reference in their concept paper.

7. Oversight is addressed

8. Build upon the NIST 800-53 suite of controls
   SDT Member comments and suggestions
   - Are there others that should be considered?
   - Drawing upon system identification by risk development working group.

- Configuration management: is the focus of CIP to address this or cyber security vulnerability? We weave these together without answering either.
- Should deal with both. Should identify separately.
- CM is a core element to what we have. Ground engineering approach in this cyber standard. What is original intent of CIP 002?
- Gaps- trying to close with CIP 002- clear path to capturing all system elements for evaluation to ensure protected at a minimal level.
- We have to get a grounding in our cyber security sector. Create a 7th element to help ensure
- One is a top down focusing on what you are trying to do, the other is bottom up. Is it best to spend resources on deciding which to protect or invest in the protection itself?
- Need to focus on differences. Look at the starting point for differences.
- Should we get away from where the vector comes in and instead look at whether there is an impact to my system?
- Strawman A focuses on control vs. addressing vulnerability.
- May not be an either/or. Create a merger between the 2.
- R1. 7 and .8 overlaps with Huff approach. Move to R4. Corollary to FIPS 199 process.
- Is there a place for R2 and 3?
- R4- merge the two. Look at 1.1. Merge the two together and discuss functional description of assets.
- Let's not talk about how. Let's focus on their function and effect on BPS. Nail this down. Then look at rest of standards. Good controls, effective, cover threats.
- Stay focused on what we should accomplish- good for cyber assets but ignore 1.1. We need to deal with these--are they in/out?
- Keep "critical assets" in there because of VSLs and compliance associated with these. Thinks merger suggestions are good.

E. Exploring the Merging of the Two Approaches- Merger Small Groups.

The facilitators suggested several discussion questions following the presentation and discussion of the strawman options including:

- What is the best place for the CIP 002 approach to start? From facilities? From Systems? From either? From both?
- What is the best approach to 3rd party oversight and accountability?
- What is the best approach to addressing external interfaces?

After some discussion, the SDT members agreed to break into two discussion groups on the morning of day two to discuss and focus on the possible merger of the approaches of the two

Strawman 002 concepts to Requirements 1 and 4. Following lunch, each group reported the results of their discussion and engaged in a full SDT discussion of the issues.

1. **Requirement #1 Small Group Report**
   (Participants: Gerry Freese, Kevin Perry, Sharon Edwards (scribe), Rich Kinas (reporter, moderator), John Lim, Jackie Collete, William Winter, David Revill and Scott Fixmer)

Rich Kinas presented to the full team a summary of the small group's discussion. The group reviewed how it would be possible to merge facilities vs. functional approach. They agreed that the starting point should be to identify the functions necessary for reliability of BES. There were questions as to whether that should be part of the standard. Some urged that there was a need to pre-define the functions. The group agreed that it would then be necessary to identify the systems or hardware used to perform those functions. It would then be necessary to incorporate the high, moderate, low threshold each into category.

SDT Member discussion comments

- Some look at systems approach vs. assets/hardware.
- Who identifies functions? It is not clear at this point would need to be addressed. It may be the SDT.
- Continue to land on fundamental differences- e.g. do we do a filter before systems assessment using BES components, or do we jump to cyber system and then roll into a component basis. May not matter that much which is the starting point. Important to get to appropriately identify systems so an entity could take either approach.
- Can we provide or point to a methodology?
- If go to a systems approach- Bill Winters might word smith an option
- Hardware-
- Define systems? Electrical vs. cyber systems.
- If "system" in R1 what is reason for R4?
- Function definition in R1 only. System to support function in R4. Keep at power stuff or functions level (e.g. AGC).
- Are reliability functions defined within reliability standards? Where is the right place to define these functions? Those requirements in operations horizon. Look for those in the High Violation risk factors?
- A control system- command and control function of controlling BES.
- Operator certification?
- Defined by other standards?
- A participant offered the following list of 9 functions for SCADA systems from their consulting work: 1. Core and Critical SCADA functions; 2. HMI & Information Network Equipment; 3. SCADA Master; Real-Time Communications Systems; 4. Data

Acquisition; 5. Automatic Generation Control; 6. Breaker Control; 7. Voltage Control; 8. State Estimation; and 9. Remote Configuration/Troubleshooting/Maintenance
- Concern about limiting to operations. Asset management. Configuration management, firm ware etc. inventory system
- SR: concept- look at already developed items to come up with a list. Look at the conceptual.
- From the R1 small group perspective: Thresholds are R3 and Cyber devices are R4.
- In the NERC Adequate Levels of Reliability document- all have standards associated with those functions.
- By using approved standards, do we have an asset list?

2. Requirement #4 Small Group Report

(Participants: Frank Kim, Phil Huff (scribe/presenter), Jeri Domingo Brewer, Scott Mix, John Varnell, Rob Antonishen, Jay Cribb, Mike Winters and Keith Stoffer

Phil Huff presented the small group's report offering the following summary points:

- The Small Group suggested taking "systems" references out of R1 and only include functions of BES in R1.
- R4 should identify the systems that support and perform the R1 functions
- Physical assets- stayed away from system categorization (R5)

3. SDT Discussion of Merging the Approaches

SDT Member Discussion Comments on Merging the Approaches

- Refreshing to see what the Strawman B did in R1- lets go forward.
- How do we identify functions? How many standards exist? About 120 standards with over 1000 Requirements. Is it realistic to point to them when defining the functions? Note, there are over 150 high risk factors.
- The OC/PC chairs- believe that the SDT is using the standards for something other than what they were designed for.
- Definition of adequate level of reliability by FERC- scope of the functions we are talking about. Characteristics.
- Concerned about ambiguity- of standard. Draft 2 of standards had numbers in it.
- Should we dictate assessment methodology in the standard?
- Standard says what- with parameters. "How" is placed elsewhere.
- Specificity has a place in certain standards. How to shed vs. when to shed.
- SDT must figure out where the specificity belongs keeping in mind that a standard is a "what" not a how. Guidelines are generally the place to lay out the "hows."
- Keep in mind we are now in the ERO era.
- Float as a white paper vs. a list of requirements?
- Adequate level of reliability paper-was it balloted?

- Will it be possible through a onetime process, to identify the functions that support the reliability of the electric system? This needs to be done. Perhaps it can be defined in standard and referred to as an appendix.
- Defining the criteria for high, mod, low, inconsequential, should be taken out of industry hands on a case by case basis and put in the standard. If REs make up their own rules, we will still have problems with consistency and uniformity of application of standards.
- The steps are: identify assets; map against functions; map against potential impact (criteria); and come up with a list of what protected to what degree.
- Don't need to define these functions- don't reiterate existing reliability standards. Cherry pick the key functions. Black and white filter may be needed here. Would simplify for end users and cut down on interpretation.
- Don't lose sight of the consensus reached in having the functions in R1, the systems in R4.
- Address the functional aspects of BES in R1. Recognize it is good to separate functional objectives of BES from systems and assets that support use.
- There is disagreement over whether the functions are defined in R1. They need to get defined as onetime process external to entities using them and then reference in standards.

F. CIP-002 Requirements 2 and 3 Critical Asset Identification Methodology (R2) and Identification (R3) Strawman

Scott Mix presented a strawman for an approach to CIP 002 Requirements 2 and 3 for consideration by the SDT. He suggested starting with functions and map to the physical equipment. Consider determining "Asset Impact" as high, moderate, low and none and "Cyber impact" as high, moderate, low and none for CIP 3-9.

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

SDT Member comments on the strawman R2 and R3 matrix

- What about load shed for economic reasons? Conceptual level
- Have to come under standards since the risk is there and need to mitigate.
- The pre-supposes a lot. Look at asset based on function and rate. Take a more systems approach tied to function. When you do categorization, look at the threat vectors.
- Very ineffective security controls may result in undermining the intent of the standard.

- **Asset based impact —** likes approach. Availability- how would loss of asset affect BES? How would misuse of system affect?
- If you look at asset before this is done, it may lead to mistakes. Take information and fold into the categorization effort.
- Shouldn't include/exclude systems with a filter/matrix.
- This will cover more systems than are covered now under the CIP.
- Developing standards guiding production systems.
- If required to have zone protections. Shouldn't design standards to accommodate
- **Remapping from function to asset —** Keep this at the function impact. You may be opening this up for avoidance behavior.
- Redundant protection is tied to the adequate level of reliability
- We haven't talked yet about oversight and wide-area view component
- Asset and function may combine — Modify- level of effort to compromise device? vs. cyber impact. Impact divided by effort? Ratio- high risk of impact, little effort to compromise. Threshold of value to provide additional protection.
- Is there a potential for "gamesmanship"? Internal actor, external actor, etc.
- Start with the function — can't secure AGC, secure computer that calculates. Need to get to functional level.
- Just do cyber impact with criteria- may not have to go through asset impact drill.
- Framework is a good thing. If you do categorization impact- after identify functions.
- **Defining thresholds —** Need to make sure we don't start putting numbers to thresholds. They may increase and then you will have to revisit to deal with the changes needed.
- Is getting down to the BES element device necessary? Keep focus on system level.
- Not excluding assets, including the system.
- "Contingency reserve"
- Added impacts into asset classification R.2.3 (get from Joe/Scott)
- Helps with appropriate levels for controls
- Relate to specific standards to give people a sense of this. Create an attachment. Binding explanation of what "significant" means.
- Put as an attachment vs. a glossary.
- Categorization?
- "Support the reliable operation of the BES". Need to clarify this.
- E.g. insignificant devise?
- What is the correlation between R2 and R3 and cyber assets in R4? Connection between R4 and R1. Moved under R4. Come into play then? Cyber approach
- R1 and R2- are generally focused on electric R4 and R5 focus on cyber.
- Each requirement by itself a simple requirement to meet.
- Break line between R3 and R4? Do both. Proposing to maintain the hierarchical order?
- Anticipating "controls"

- Are these exclusive. Do we need R2 and 3 any more? Can't apply a control to a function.
- Control framework- requirements 003-009. NIST calls security controls. NERC
- Hierarchal ranking of assets-
- Look at functions, correlate to cyber systems, apply controls 003-009
- Without an engineering review of impact- R2.3 do it as overt operation that can be audited.
- Put in the relevant detail. Don't do before you know what cyber assets perform what functions.
- R2 and R3 are top down. Does each requirement stand alone? Each is building as a filter or additive. If leave out 2 and 3, then you can't build later the matrix.
- This may allow RE pick and choose and make up own rules? If we can define the threshold criteria identification importance. If you want RE to do, then leave 2 and 3 in. Determine in an appropriate manner.
- R 2.3 process. IROL caused by cyber asset? If remove R2.3- won't
- Pre suppose cyber assets everywhere.
- R1 now. Most are systems. R2 and R3 is part of categorization process. Need engineering criteria in R5.
- Use matrix approach — complex- 16 cells. Meld to high medium low or none.
- Options include: 1. Keep R2 and R3; 2. Keep with SM's language; 3.Move
- Need to clarify what "cyber impact" means. Cyber impact on a particular asset? Include going forward- components of connectivity, impact of cyber system on asset/function.
- Supports a 2 dimensional matrix.
- R2 and R3 — captured in the external engineering studies on Strawman A flow chart. Not a requirement in this because it would be done externally. R2 and R3 performed external to the entity process.
- Impact assessments: need to keep separate? Performing 1 impact analysis.
- Haven't had good results in getting new methodology out to the industry quickly. Will any of these be better than what we have today? Looking for more consistent answers from each utility.
- Similar enough to be the same flow chart. Are they the same flow if you move that one box?
- Is there agreement with moving the arrow will result in no 2 dimensional matrix? Cyber impacts may have not bearing on the functions.
- Cyber impact assessments — consider impact on physical assets of BES due to impacts of a cyber asset?
- Breaker control relay- cyber asset impacts the breaker associated with.
- What is a cyber impact? Impact on the BES. Independent of impact on physical asset that it is controlling? Why bother generating list of cyber assets for low impact? Low but some level of protection.
- Impact on that asset and impact on BES comes in through the matrix.

- We are looking at this from bottom up and top down.
- Left side of flow chart covers the impacts and consequences. Right side- cyber impacts as a vulnerability assessment. What kind of connectivity does it have etc. Sounds like 2 pieces of a risk score. Take the controls and apply to.
- Cyber impact is the impact to the operation of the specific asset using vector of protected system- does it cause the engineering asset to misbehave.
- We are struggling with a difference in terminology. Cyber impact on the Strawman B chart is blind to the broader system. Impacts on the Strawman A chart take holistic view of the system.
- Is the difference a vulnerability vs impact assessment?
- What happens with malicious behavior?
- Part of cyber assessment — assess use of un-authenticated relay.
- Interpretation of cyber impacts — what is the reach of cyber assets- how many units can it kill. How bad can it make things from its viewpoint?
- Should we make a decision based on that impact-
- Common mode impact from the guideline and put in standard to be become binding?
- Cyber impacts- how they impact the BES.
- Vulnerability assessment to R5-

The facilitators suggested polling on three proposals for going forward that emerged from the discussions:

Proposal 1 Keep R2 + R3 with Scott's Language (Matrix)
Proposal 2 Move R2 & R3 into R5 (Vector Analysis)
Proposal 3 R2 + R3 Performed by External Entity

1. **Proposal #1: Keep R2 + R3 with Scott's Language (Matrix)**

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.*
Proposal 1- R 2& R3	**6**	**5**	**6** (5/1)	**1**	**2.9 of 4**

Comments after ranking:

- #1s: This is not right framework- misplaced. Concept of keeping R2 and R3. Placement is a big deal
- #2s: not convinced complexity of 2 way matrixes is necessary.
- #2s splitting the assessments — what physical are you looking at? Cyber impact doesn't have meaning within methodology.
- #2s Not seeing the meaning of the cyber impact assessment

- #2sTaking us as group we are not on the same page- we will have difficulty pushing concept to industry.
- #2sWhat if we split this into 2 analyses. May be a lot of work that may not matter in the long run. Better to have in 1 integrated process. Bring all into 1 assessment process.

SDT Comments

- Important to be clear about ultimate requirements that we write.
- Cyber impact- left hand side- what happens if BES asset is compromised, goes away.
- Right hand column- cyber impact- what bad things could be done with device if it were compromised on the target of evaluation.
- Next version of standards- keeping R2 and R3 asset ranking is necessary. Applying more gradations vs. roll into big process with cyber impact. Industry might prefer to keep 2 & 3.
- Didn't vote- didn't get any sense of a system- in this.
- Is the process based on theory? Why you can't take last arrow and connect to impact- not mapping functionally? What is the cyber assessment. Other flow chart- engineering studies.
- Ranking based on reality-
- Risk vs. impact analysis- e.g. vulnerabilities.
- Are we ever going to bring in vulnerability?—yes, when we get to 003-009 for the control selection phase but we have to determine how many and how tough need to be.
- Analogy- FIPS 199- before categorize, incorporate risk assessment and existing plan and previous assessment. Impacts how you rate the system. Impact has no meaning if you don't have risk appetite. Audited for insufficient risk assessment before categorize system- and picking controls.

2. Move R2 and R3 to R5 for a single vector analysis- concept

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.*
Proposal 2- R 2& R3	**4** (3/1)	**5**	**9** (8/1)	**0**	**2.7 of 4**

Member comments after ranking

- 2's: value in evaluating BES independently of the cyber assets. May be easier for industry to get head around. May help with other standards.

3. Have R2 and R3 Performed by External Entity

Acceptability Ranking Scale	*4 = acceptable, I*	*3 = acceptable, I agree with minor*	*2 = not acceptable unless major reservations*	*1 = not acceptable*	*Avg.*

	agree	*reservations*	*addressed*		
Proposal 2- R 2& R3	**1**	**0**	**9**	**5**	**1.8 of 4**

G. Developing A Common Framework

At the end of the second day, a small group agreed to work further on a draft common framework. The group included Phil Huff, John Lim, Scott Mix, Jackie Collett, Scott Rosenberg and John Varnell. Jackie Collett introduced a flow chart as a strawman designed to be flexible to allow for further development and refinements. She understands that it will be important to clear up terminology so references are understood. Phil Huff offered that this concept captures the focus on cyber systems (not on assets) and does not offer a hierarchal model. The "vector" categorization- matrix offers some more granularity as to what we are meaning to accomplish. It offers a cyber impact analysis of impacts on the function. Still performing the same transitive impact analysis that is logically equivalent.

Concept

Identification of BES functions which support the reliability and operability of the BES

Need 1 layer of specificity below ALR

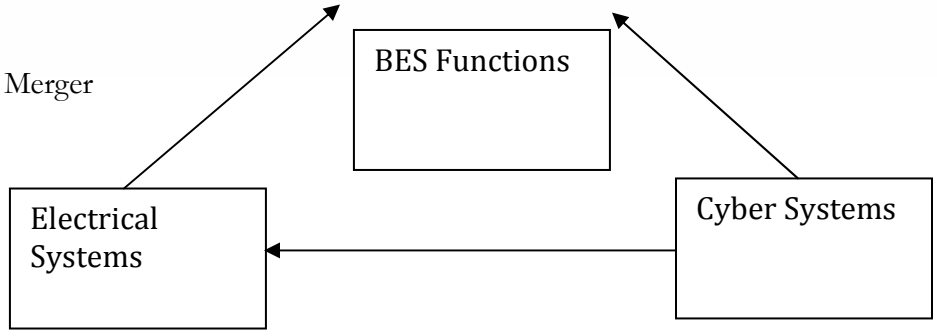
Cyber Impact — the local impact due to loss of CIA of the cyber asset for a BES element

System — a set of components which must work together

Electric System — a set of BES elements which must work together

Cyber System — a set of cyber components which must work together

Pre-Determined Functions			
R1	List of Electric Systems which support the BES functions	R4	List of Cyber Systems which support the Electric Systems and/or BES Functions
R2	Method of Categorization - impact to BES	R5	Method of Categorization - local impact to Electric System components
R3	List of Systems & Categories	R6	List of Systems & Categories
R7	Matrix: combines the 2 impact levels		
R8	Local Approval		
R9	Oversight		



Member comments on the Concept

- Is the definition of a cyber incident being only local? Does this suggest any difference of between cyber and electric.
- Haven't yet defined criteria. Connectivity on the cyber side might fit. They don't map well together. Cyber asset impact side put something in on connectivity.
- SM: formative stages. Focusing on local BES impact from a cyber stand point. Open to addressing network interconnectivity. Detail to be fleshed out later.
- Clarification- which bucket would a sweitzer 100 series relays (with a micro processor) fall in? What would industry think. Clarify what is a cyber asset. Helpful to have a one page on the guiding principles for the CIP effort.
- Network connectivity — weigh in on the cyber impact analysis
- Right side- call "control system" vs. "cyber system"? Direction can provide clarity. However, puts you in the weeds quickly.
- What is the object of the requirements?
- Terms should be fairly self explanatory. Not only systems that control, but also coordinate, alarm, situation awareness.
- Terminology- from different niches- "cyber" system is problematic. Move away from it.
- Go to control systems- nested definition sequence. Look at those definitions from Strawman A.
- Decouple- like the fact there is no discriminating filter. Solves that problem. Not convinced 2 matrixes. Willing to see how progresses. Key point in Huff approach-
- Detail didn't get to last night. There will be an oversight component. Difficult for 2 entities to talk with each other.
- Get captured in the pre determined function list that is built- e.g. exchange of data could be a function unto itself.
- System selections identified. Is intent to end with a list of systems that we've established an impact level of? Then identify elements you have to apply to? Put into additional CIP requirements.

- Don't part the sheep's from goats, blanket that covers everything but focuses attention are areas for greatest impact. May take 10-15 year timeframe to get there. There is a pile of assets we should worry about fixing in 2 years. Next level- have 5 years to do something with applying a lesser set of controls to a broader family of systems; another layer taking 10 years to get all of those done. At end, broad scope of coverage.
- How big a blanket? No agreement yet. However, more protection that what is currently implemented today.
- Identify an implementation time frame that would be reasonable to the industry.
- Use definitions- Alphabet soup draft- Cyber asset, system control systems.
- Any device that is programmable is in scope.
- Careful about using terms, mixing them up. Makes it confusing. Need come up with terms we agree on.
- Terminology-- careful we don't reuse terms- e.g. critical asset. Inventing new terms and using consistently. Do this sooner vs. later. NERC glossary — e.g. element.
- Note that this is a work in progress.
- Drafting team glossary before the next meeting. Beneficial.
- R1-3 pieces as planning type elements. R4-6 micro processor. Don't mix initially. Then combine.
- Other advantage — FERC 706 order — oversight is on the electrical side not on the cyber side. That's where there is oversight authority related to BES.
- "Big Iron" piece.
- Appreciation for this work. This concept is a benefit to entire effort. CIP standards are incomplete. Physical side needs to be developed. Leaves in that side that will address the physical side for the next SAR. I Like this.
- R1 and R4- how to scope down so not lists of 10 million? Will be scoped down on the identification of BES functions. "Generation control"
- Functions will be "pre determined" by the SDT.

Following the discussion the SDT agreed to rank the acceptability of the following proposition:

Adopt as a working conceptual model for SDT to develop frame and concept paper that includes a set of definitions/glossary, Develops a list of functions and uses list of scenarios to test the concept.

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.*
3-12 SDT rank	**15**	**3** *(1/2)*	**1**	**1**	**3.6 of 4**
Second Rank with D Norton's Concept	**15**	**3**	**2**	**0**	**3.65 of 4**

Comments after the ranking

- Dave Norton ranked this with a 1 and explained it by presented a flow chart he had been working on *(See Appendix #9)* that was titled "Scoping Logic Synthesis Proposal"
- Rich Kinas gave it a 2 indicated his preference would be to create and compare a range of multiple competing approaches before settling on a framework for Phase 2.
- Voted 3: those working with both federal and NERC compliance at same time may find it hard to look at reliability from a cyber perspective- need to put in context. Hard for understanding each other. Federal experience suggests we will have a hard time with this.
- If on the cyber side we do a good job = functional description of systems and how relate to functions of BES.
- Good controls on cyber system to minimize risk. Demonstrate positive impact on BES. Setting stage for better dialogue with the industry.
- Could make it worse than now but on balance this is a good positive step.
- Voted 3- Shared Rich's view point. Taken aback- on the complexity of matrix approach. Left hand side- look to planners how are these falling out. Cyber side is right hand side is what is depicted. Complexity is an issue. Perception that standards are unnecessarily complex and wastes time. The more direct we make this the better.
- We can incorporate Dave Norton's ideas into this model. E.g. system restoration? Right hand or left side? Functions.
- There are lots of options but we should do something with this and see if it makes sense, see how this actually work in practice.
- DN ideas might fit in R4-6. Add this in.
- Standards should help provide everything in BES needs to be protected at some level.
- Engage in DN's next about how left and right side map.
- Voted 4 because it is a concept. DN's proposal is CIP 002 supported by concept paper. Where the criteria gets set is key. If criteria for categorizing set externally to RE, then single column can work and simplify the process.
- If RE's continue to make own rules, will strive to make low or none and it is hard
- R 1-3 what is the product of that? BES inventory run. Categorizing now with N-1, list will be automatically high. Leads to maximum controls. R3 is the documentation.

In the discussion of the approach going forward concern was expressed about whether the SDT was the right group to develop the concepts for Requirements 1,2, and 3 (the left hand side). Planning and operations perspectives would be helpful. The current SDT is 90% cyber folks. Dave Taylor volunteered and the SDT agreed that he should draft a white paper to present to the next meeting on a process for determining Requirements 1, 2 and 3.

Bill Winters requested the SDT rank the following proposition that if acceptable would be incorporated into the white paper going forward as the CIP 002 intent statement:

CIP 002 is intended to provide a discovery methodology that will lead to explicit identification and categorization of all cyber elements that <u>performs or supports</u> BES functions.

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.*
3-12 SDT rank	**18** (16/2)	**1**	**0**	**0**	**3.9 of 4**

VI. NEXT STEPS and Assignments

A. Drafting Assignments

The SDT agreed that a helpful next step would be to refine the concept presented and tested on the third day in the form of a draft white paper. The chair asked Jackie Collett, John Lim, Bill Winters and Phil Huff along with Scott Mix to take the lead in the development of the draft white paper in advance of the April meeting building on the discussion and outcomes of this meeting. Other members would be welcome to send ideas and reactions as well as listen in and participate on the webex meetings that would be convened. The goal would be to be able to share the white paper with the industry following either the May, 2009 or June, 2009 meeting.

B. SDT Meetings Schedule, 2009

The SDT members completed calendar forms regarding possible dates for future SDT meetings. Upon review of the forms and SDT member scheduling conflicts, the following dates and tentative locations were established and agreed to by the team.

Proposed Dates and Locations for Future Meetings 2009

Dates in 2009	Location
April 14–16	Charlotte, NC
May 13–14	Boulder City, NV
June 17–18	Portland, OR
July 13–14	Toronto, CA
August 20–21	Chicago, IL
September 9–10	Denver, CO
October 20–22	New Orleans, LA
November 17–18	Atlanta, GA
December 15–17	Key West or FRCC (Tampa, FL)

The SDT agreed to seek to make a progress report to the MRC at its May meeting in Arlington, Virginia and provide a substantive briefing on the Phase II white paper for input at their August meeting.

The team discussed the timing and objectives for a workshop. Some members suggested it could be an opportunity to brief on the Phase II approach and receive input from experts from other standards bodies as well as FERC and Congressional members and staff. The chair noted that the NERC standards committee had carefully selected subject matter experts to serve as members.

The SDT decided to hold open the question of convening an expert/stakeholder workshop pending the Chair and Vice Chair's discussion with Michael Assante, NERC Chief Security

Officer, to gain a clearer understanding of the potential objectives, design and timing of a workshop in light of the SDT's progress and schedule.

C. Meeting and SDT Process Evaluation
The facilitators offered some observations on the SDT's team work over the past six months including:

- The SDT 706 team is larger that many SDTs
- The issues under review are complex and contentious technical and operational issues
- Contentious
- The members are highly knowledgeable and articulate with strong opinions.
- There has been measurable progress in proceeding on a two phase approach to their work.
- There has been a helpful sharing among the team members on what has been working and constructive suggestions on what could be improved.
- The facilitators should help to clarify within meetings the objectives sought for each session and check on the chair's, vice chair's and the team's sense of whether they have been met before transitioning to other sessions.
- The team members often in the context of reviewing and debating key issues will use experiences to illustrate points or test proposition which takes time and in some instances may not advance the discussion.
- The team and facilitators have been sensitive to the "violent agreement" rule but may need to manage that more assertively so that members know that it is being captured in the record and there may not be a need to repeat.

The facilitators suggested and the Chair and team agreed that it would be timely to survey the Team on the experience over the past six months to provide an opportunity for deeper shared reflections on the ways to improve the team's process.

The SDT adjourned at 11:45 a.m. on March 12.

Appendix 2 — Meeting Attendee List

Attending in Person — SDT Members

1. Rob Antonishen	Ontario Power Generation
2 Jeri Domingo-Brewer, Chair	**U.S. Bureau of Reclamation**
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Information Security Analyst, Southern Company Services, Inc.
5. Sharon Edwards	Duke Energy
6. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
7. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
8. Phillip Huff	Arkansas Electric Coop Corporation
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
10. Frank Kim	Ontario Hydro
11. Richard Kinas	Orlando Utilities Commission
12. David Norton	Policy Consultant, CIP Energy Corporation
13. **Kevin B. Perry, Vice Ch.**	Director, IT-Infrastructure, Southwest Power Pool
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy
16.Keith Stouffer	National Institute of Standards & Technology
17. John D. Varnell	Technology Director, Tenaska Power Services Co.
18.Michael Winters	Ontario Hydro
19.William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	*NERC*
2. David Taylor	*NERC*
3. Scott R. Mix	*NERC*
4. Joe Bucciero	*NERC/Bucciero Assoc.*
6. Robert Jones	*FSU/FCRC Consensus Center*
7. Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

20. Tom Hoffstetter	Midwest ISO, Inc
21. Kevin Sherlin	Sacramento Municipal Utility District
22. 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

Others Attending in Person

Jim Breton	ERCOT
Roger Fradenburgh	Netsecctech
Judy Fry	ICFI
Darren Highfill	ENERNEX

Sam Morrell	CERT
Farzaneh Tafreshi	ICFI

Others Attending via WebEx and Phone

Chris Wright	
Dan Mishra	
David Batz	
Monica Coflin	
Karen Yoder	

Appendix 4 — Michael Winters Note to SDT

From: **WINTERS Michael**

To: **'CS_706_SDT@NERC.COM' <CS_706_SDT@NERC.COM>**

Sent: **Thu Mar 12 07:27:27 2009**

Subject: **All the best Fellow SDTers –**

I had to leave prior to us finishing up yesterday so I didn't get a chance to say goodbye.

It has been a pleasure working with each of you and being a part of this very important team. It goes without saying that these standards are much needed in our industry and the direction you are taking them is a good one. They have already served to introduce good information technology practices into power system engineering. These practices need to be applied at different degrees to all cyber assets used for power system operations (or at least allow for an explicit and auditable decision to not apply them to some assets).

I have learned a significant amount as part of this team and for that I thank you. I look forward to seeing where you take us.

All the best, Mike

Appendix 5

Cyber Security Order 706 SDT — Project 2008-06
January through June 2009 Draft Schedule

Short Term 2009 SDT Schedule Draft Criteria

- Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
- Seek creative ways to get advice and input to the SDT from experts in cyber security.
- Seek creative ways to get focused input from industry stakeholders.
- Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
- Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
- Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cyber security for the 44th President.

SDT Draft Schedule — January through June 2009

OVERVIEW

- 7 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommittees WebEx Meetings
- 1 Cyber Expert Workshop (March 10 or 11, 2009)
- 1 NERC CIPC presentation? (February 9, 2009)
- Industry Comments on CIP-002 White Paper (April 17 through June 3)
- 1 NERC Members Representative Committee, May 1, 2009
- Other Meetings?

1. **January 7–9, 2009 Meeting in Phoenix, AZ —** half, full, half day format **—** Wednesday through Friday
   - Review of Technical Feasibility Exceptions white paper
   - Review of Industry Comments on Phase 1 products- Establish and convene small groups
   - Review of Phase 2 White papers

January 15 WebEx meeting(s)

- Small group draft responses to industry.

- Phase 2 drafting concept group?

January 21 WebEx meeting(s)
- Small group draft responses to industry.
- Phase 2 drafting concept group?

2. **February 2–4, 2009 Meeting in Phoenix, AZ — half, full, half day format — Monday through Wednesday**
   - Review of Industry Comments on Phase 1 products and proposed revisions and adoption of Phase 1 products.
   - Review of Phase 2 White papers and Testing of a Phase 2 CIP-002 Concept going forward

February 9, 200 — CIPC Meeting — Update on SDT Progress and Input

3. **February 18–19, 2009 Meeting in Boulder City, NV**
   - Review of Phase 2 White papers and Adoption of a Phase 2 CIP-002 Concept for review by experts and stakeholders

February 25 WebEx meeting(s)
- Development of Phase 2 CIP 002 Workshop for review by experts and stakeholders

4. **March 10–11, 2009 Meeting in Tampa, FL, 2-day format**
   - **Invited Cyber Security Experts join SDT in a workshop** to provide expert feedback to draft CIP-002 concept.
   - Further SDT refinement of the CIP-002 proposed concept

March NERC Balloting on Phase 1 Products

March 18, Webex meeting(s)
- Phase 2 drafting concept group?

5. **April 14–16, 2009 Meeting in Charlotte NC — half, full, half day format — Wednesday through Friday**
   - Continue review and refinement of CIP-002 concept
   - Adopt White Paper on CIP-002 concept for Industry Comment

Industry Comment Period on White Paper — 45-days (April 17 through June 3)

*May 1, **NERC Member Representative Committee**, Presentation of the Phase 2 CIP-002 Approach for MRC input. (Agenda item, Possible Workshop?)*

6. May 13–14, 2009 Meeting in Dallas TX — 2-day format

- Respond to MRC input and further SDT refinement of the CIP-002 proposed concept and SDT CIP roadmap.
- Organize SDT in subcommittees to draft revisions to CIP-003-CIP-008 or to address key issue areas.

Early June WebEx meeting(s)

- SDT subcommittee meetings to review and draft responses to Industry comments on the CIP-002 concept.

7. June 17–18, 2009 Meeting — Location TBD — 2-day format

- Review Subcommittee responses to Industry comments on CIP-002 approach
- Charge subcommittees and conduct organizational meetings
- Subcommittees meet to draft revisions to CIP-003-CIP-008

June, 2009 WebEx meeting

- SDT Subcommittee meetings

July–December, 2009 — SDT and subcommittees meet and continue CIP drafting

Second Draft Phase 2 Roadmap Approach Assessment Criteria
(Presented, Revised and Added to by SDT in its review on November 14, 2008)

1. The approach is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
2. The approach is achievable given the SDT schedule and work plan.
3. The approach does most to advance and enhance cyber security in the BES.
4. The approach helps the SDT address the foundational issues with the current standards.
5. The approach is capable of implementation.
6. The approach is capable of improving compliance.
7. The approach helps protect the current investments and wherever possible builds on what has already been done.
8. The approach helps to identify and mitigate risk on an ongoing basis.
9. The approach balances a “systems” orientation with a “facilities” orientation to asset protection.
10. The approach is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).

11. The approach enables the industry to provide the appropriate level of security (i.e. not over securing nor under securing the BES cyber assets).
12. The approach allows for discrimination among and targeting the various types of infrastructure that support the BES

Appendix 6 — CIP-002 Strawman A

(Phil Huff, Jeri Domingo Brewer, Kevin Perry, Keith Stoffer, and Bill Winters)

Definitions:

Cyber Asset — Programmable electronic devices and communication networks including hardware, software, and data. [NERC Glossary]

Cyber System — A discrete set of Cyber Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Adapted from NIST SP 800-53 definition of Information Systems]

Control Systems — computer-based facilities, Cyber Systems, and equipment used to remotely monitor and control sensitive processes and physical functions. These systems collect sensor measurements and operational data from the field, process and display this information, then relay control commands to local or remote equipment. [Joint DOE/DHS Roadmap to Secure Control Systems in the Energy Sector – January 2006]

B. Requirements

R1. The Responsible Entity shall produce through an annually applied process, a list of Cyber Systems that are to be protected per the requirements of the CIP standards. The Responsible Entity shall at least annually:

R1.1. Identify all Control Systems that perform supervisory control functions (e.g. open/close breakers, raise/lower generation) for the Bulk Electric System or provide situational awareness of the state of the Bulk Electric System. This would include:

- Systems that provide situational awareness
- Systems performing EMS/SCADA functions
- Special Protection systems
- Systems essential to BES restoration
- Systems performing automatic load shedding
- Other systems that may perform a function directly related to BES system reliability

R1.2. Identify internal and external data interconnections between Cyber Systems that provide data necessary for the reliability functions of the previously identified Cyber Systems or Control Systems.

R2. The Responsible Entity shall define one or more security boundaries to encompass the identified Cyber Systems.

R3. The Responsible Entity shall review, update as necessary, and obtain Regional approval of its Cyber System categorization criteria at least once every three years.

R4. The Responsible Entity shall annually categorize each identified Cyber System as low, moderate, or high potential impact to the Bulk Electric System using Regionally-approved categorization criteria. The categorized list shall reflect the importance of integrity, availability, and confidentiality the Cyber System or data and the potential risk to the reliability of the Bulk Electric System in the event the Cyber System is lost or compromised.

R5. The Responsible Entity shall evaluate and categorize new and replacement Cyber Systems using the applied process and categorization criteria prior to being placed into service.

R6. The Responsible Entity shall designate a senior manager with the responsibility and authority to approve the categorized list of Cyber Systems.

R7. The Responsible Entity shall communicate and coordinate with the external Responsible Entity any identified external data interconnections between Cyber Systems and the potential impact to the reliability functions of the Responsible Entity.

Appendix 7 — CIP-002 Strawman B
(John Lim, Jackie Collett, Scott Rosenberger, and John Varnell)

Introduction

Title: Cyber Security — Cyber Asset Identification and Categorization

Number: CIP-002-3

Purpose: NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification, categorization and protection of Cyber Assets to support the reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification, categorization and documentation of the Cyber Assets associated with the Assets that support the reliable operation of the Bulk Electric System. These Assets are to be identified and categorized as Critical and non-Critical based on the application of an impact assessment.

Applicability:

Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

Reliability Coordinator.
Balancing Authority.
Interchange Authority.
Transmission Service Provider.
Transmission Owner.
Transmission Operator.
Generator Owner.
Generator Operator.
Load Serving Entity.
NERC.
Regional Entity.

The following are exempt from Standard CIP-002-2:

Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

Effective Date:

The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Requirements

R.1 Identification of BES Assets – The Responsible Entity shall identify and document a complete list of BES Assets. Assets may be identified as facilities, equipment or systems. The Responsible Entity shall include, wherever applicable, the following:

Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

Transmission substations that support the reliable operation of the Bulk Electric System

Generation resources that support the reliable operation of the Bulk Electric System.

Systems and facilities used for system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more

Special Protection Systems that support the reliable operation of the Bulk Electric System.

Systems that support wide-area reliability through one or more of the following:

Situational awareness
Supervisory and control capability
Other systems that may perform a function directly related to the reliability or operability of the BES.

Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

Critical Asset Identification Method — The Responsible Entity shall identify and document an impact assessment methodology to use to identify its Critical Assets.

(Note: This requirement assumes that the NERC guideline will provide more specific guidance in the development of the methodology. As suggested by Scott Mix, a change in terminology may reflect more accurately the nature of this methodology.)

The Responsible Entity shall maintain documentation describing its impact assessment methodology that includes procedures and evaluation criteria. The evaluation shall include consideration for Common Mode Impact and Adequate Level of Reliability.
The impact assessment shall be applied to the BES Assets identified in R1.

Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the impact assessment methodology required in R2. The Responsible Entity shall review this list at least annually, and update it as necessary.

Cyber Asset Identification — Using the list of Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Cyber Assets essential to the operation of the BES Assets.

Cyber Assets which support the following shall be included:

The operation and control of these BES Assets

The monitoring and alerting functions for the reliable operation of these BES assets

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

Any cyber asset which directly interfaces with these Cyber Assets, and which is not identified as a Cyber Asset performing the functions in R4.1 on a BES Asset, will be identified.

The intent here to identify cyber assets which interface with BES Cyber Assets, in most cases for providing data for non-realtime analysis (such as PI data servers or data base servers. These may warrant adequate protection because of their relationship with BES Assets.

The Responsible Entity shall review this list at least annually, and update it as necessary.

Huff R1.1. Identify all Control Systems that perform supervisory control functions (e.g. open/close breakers, raise/lower generation) for the Bulk Electric System or provide situational awareness of the state of the Bulk Electric System. This would include:

Systems that provide situational awareness

Systems performing EMS/SCADA functions

Special Protection systems

Systems essential to BES restoration

Systems performing automatic load shedding

Other systems that may perform a function directly related to BES system reliability

Huff R1.2. Identify internal and external data interconnections between Cyber Systems that provide data necessary for the reliability functions of the previously identified Cyber Systems or Control Systems.

Categorization of Cyber Assets — The Responsible Entity shall apply the following criteria to categorize the identified Cyber Assets:

(In a perfect world, entities should be allowed to determine on their own which cyber assets are high, medium or low. Unfortunately, the current enforcement model does not lend itself to this kind flexibility and requires a more prescriptive categorization scheme.)

High Impact Cyber Assets — All identified Cyber Assets which perform the functions in R4.1 for Critical Cyber Assets shall be included in this category.

Other High Impact Cyber Assets may be identified as a result of further standards.

Medium Impact Cyber Assets — All identified Cyber Assets which directly interface with a High impact system in a protected ESP is a Medium impact cyber asset. Interface is defined as an application based data exchange across an ESP access point.

(Note: Other Medium Impact Cyber Assets will be categorized when the ESP is defined as part of CIP-005 and “incidental” cyber assets in the same perimeter as High Impact cyber assets will be categorized as Medium Impact systems).

Low Impact Cyber Assets — Any cyber asset not categorized as either High or Medium Impact shall be categorized as a Low Impact Cyber Asset.

Annual Approval — The senior manager or delegate(s) shall approve annually the impact assessment methodology, the list of Critical Assets and the list Cyber Assets and their categorization. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the impact assessment methodology, the list of Critical Assets and the list of Cyber Assets and their categorization.

Appendix 8 — CIP-002-3 Strawman (Scott Mix)

Standard CIP–002–3 — Cyber Security — Cyber Asset Identification and Categorization

A. Introduction

1. **Title:** Cyber Security — Cyber Asset Identification and Categorization

2. **Number:** CIP-002-3

3. **Purpose:** NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification, categorization and protection of Cyber Assets to support the reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002-3 requires the identification, categorization and documentation of the Cyber Assets associated with the Assets that support the reliable operation of the Bulk Electric System. These Assets are to be identified and categorized as Critical and non-Critical based on the application of an impact assessment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

   - **4.1.1** Reliability Coordinator.
   - **4.1.2** Balancing Authority.
   - **4.1.3** Interchange Authority.
   - **4.1.4** Transmission Service Provider.
   - **4.1.5** Transmission Owner.
   - **4.1.6** Transmission Operator.
   - **4.1.7** Generator Owner.
   - **4.1.8** Generator Operator.
   - **4.1.9** Load Serving Entity.
   - **4.1.10** NERC.
   - **4.1.11** Regional Entity.

   4.2. The following are exempt from Standard CIP-002-2:

   - **4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
   - **4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Author
Comment: NEED NRC language – Systems …

Author
Comment: Need to determine how to eliminate this clause

Strawman – March 2009 – Collett, Lim, Rosenberger, Varnell
1

B. Requirements

R1. Identification of BES Assets – The Responsible Entity shall identify and document a complete list of BES Assets. Assets may be identified as facilities, equipment or systems. The Responsible Entity shall include, wherever applicable, the following:

Author
Comment: How to determine?

R1.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2. Transmission substations that support the reliable operation of the Bulk Electric System.

Author
Comment: How to determine?

R1.3. Generation resources that support the reliable operation of the Bulk Electric System.

Author
Comment: How to determine?

R1.4. Systems and facilities used for system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

Author
Comment: How to determine?

R1.7. Systems that support wide-area reliability through one or more of the following:

R1.7.1. Situational awareness

R1.7.2. Supervisory and control capability

R1.7.3. Other systems that may perform a function directly related to the reliability or operability of the BES.

R1.8. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification Method — The Responsible Entity shall identify and document an impact assessment methodology to use to *classify* ts Critical Assets *based on each asset's impact to reliable operations of the BES*.

Author
Deleted: identify i

(Note: This requirement assumes that the NERC guideline will provide more specific guidance in the development of the methodology. As suggested by Scott Mix, a change in terminology may reflect more accurately the nature of this methodology.)

R2.1. The Responsible Entity shall maintain documentation describing its impact assessment methodology that includes procedures and evaluation criteria. The evaluation shall include consideration for Common Mode Impact and Adequate Level of Reliability.

R2.2. The impact assessment shall be applied to *all* BES Assets identified in R1.

Author
Deleted: the

R2.3. The impact assessment shall describe methods or thresholds for assigning one of the following impact levels to each asset:

Author
Formatted: Bullets and Numbering

- *High Impact – loss damage or misuse of the identified asset results in significant impact or significant potential impact to reliable operations of the BES*
- *Medium Impact – loss damage or misuse of the identified asset results in moderate impact or significant potential impact to reliable operations of the BES*
- *Low Impact – loss damage or misuse of the identified asset results in minimal, but identifiable, impact or potential impact to reliable operations of the BES*

Author
Comment: need to define

Author
Comment: need to define

Author
Comment: need to define

- *No Impact – loss damage or misuse of the identified asset results in no identifiable impact or potential impact to reliable operations of the BES*

R3. Critical Asset Identification — The Responsible Entity shall develop a list of its Critical Assets *and their impact classification, as* determined through an annual application of the impact assessment methodology required in R2. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3.1. *The resultant list shall include both the identification of each Asset, as well as its classification level using the impact levels described in Requirement R2.3*

R4. Cyber Asset Identification — Using the list of Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Cyber Assets essential to the operation of the BES Assets.

R4.1. Cyber Assets which support the following shall be included:

R4.1.1. The operation and control of these BES Assets

R4.1.2. The monitoring and alerting functions for the reliable operation of these BES assets

R4.1.3. The data acquisition equipment and systems which support automated or operator assisted real-time reliable operation of these BES assets

R4.2. Any cyber asset which directly interfaces with these Cyber Assets, and which is not identified as a Cyber Asset performing the functions in R4.1 on a BES Asset, will be identified.

The intent here to identify cyber assets which interface with BES Cyber Assets, in most cases for providing data for non-realtime analysis (such as PI data servers or data base servers. These may warrant adequate protection because of their relationship with BES Assets.

R4.3. The Responsible Entity shall review this list at least annually, and update it as necessary.

R5. Categorization of Cyber Assets – The Responsible Entity shall apply the following criteria to categorize the identified Cyber Assets:

(In a perfect world, entities should be allowed to determine on their own which cyber assets are high, medium or low. Unfortunately, the current enforcement model does not lend itself to this kind flexibility and requires a more prescriptive categorization scheme.)

R5.1. High Impact Cyber Assets - All identified Cyber Assets which perform the functions in R4.1 for Critical Cyber Assets shall be included in this category.

Other High Impact Cyber Assets may be identified as a result of further standards.

R5.2. Medium Impact Cyber Assets – All identified Cyber Assets which directly interface with a High impact system in a protected ESP is a Medium impact cyber asset. Interface is defined as an application based data exchange across an ESP access point.

(Note: Other Medium Impact Cyber Assets will be categorized when the ESP is defined as part of CIP-005 and "incidental" cyber assets in the same perimeter as High Impact cyber assets will be categorized as Medium Impact systems).

Author
Deleted: identified

Author
Comment: how to identify?

Author
Formatted: Bullets and Numbering

Author
Comment: how to identify?

Author
Comment: 2-step process: Cyber asset impact AND Cyber-asset-impact to Asset impact

R5.3. Low Impact Cyber Assets – Any cyber asset not categorized as either High or Medium Impact shall be categorized as a Low Impact Cyber Asset.

R6. Annual Approval — The senior manager or delegate(s) shall approve annually the impact assessment methodology, the list of Critical Assets *and their categorization,* and the list Cyber Assets and their categorization. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the impact assessment methodology, *a signed and dated record of* the list of Critical Assets and *a signed and dated record of* the list of Cyber Assets and their categorization. *The Region / RC must approve the methodology and list of Assets and their characterization.*

Author
Comment: Need external oversight and approval per FERC order

Scoping Logic Synthesis Proposal