NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

July 13, 2010 | 8 AM to 5 PM PST
July 14, 2010 | 8 AM to 5 PM PST
July 15, 2010 | 8 AM to 5:00 PM PST
July 16, 2010 | 8 AM to 12:00 PM PST

Adopted Unanimously August 12, 2010

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

Joe Bucciero, Bucciero Consulting, LLC

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT July 13-16, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT JULY 13-16, 2010 MEETING
CERT Software Engineering Institute, Carnegie Mellon University
Pittsburgh, PA

EXECUTIVE SUMMARY

On Tuesday morning, the Chair, John Lim and Vice Chair Phil Huff welcomed the members and participants to the SDT's 24th meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The host Sam Merrill, a participant in the SDT sub-team process, welcomed everyone to the facilities and covered logistics. Bob Jones, facilitator, reviewed the proposed meeting agenda. On Wednesday afternoon the SDT approved without objection the meeting summary for the June 8-11, 2010 SDT session in Sacramento, California. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines each day of the meeting.

The Chair noted that the Team had met by conference call/ready talk three times since the Sacramento meeting to review and adopt a revised schedule to produce, ballot and send on to FERC a narrowly framed CIP 002-4 by the end of 2010. He also pointed out that the draft agenda sent out the week before has been revised based on member feedback so that the Team will be meeting together in a plenary format until at least Thursday.

The Vice Chair, Phil Huff noted the inclusion of "lunch and learn" sessions that are intended to present helpful additional information and briefings as requested by the Team.

The Chair and Vice Chair introduced the challenge of functioning with 26 members and an 18-member quorum to conduct business. After discussing the pros and cons a straw poll was taken of those members in favor of changing quorum in which 4 were in favor and 16 opposed. Following the straw poll the motion was withdrawn. A second proposal was offered for changing 75% decision rule to 2/3's. After discussing the pros and cons a motion was made to change the 2/3 decision voting rule for the SDT to 2/3s from the current ¾ and 17 members voted in favor with 3 opposed (85%) which passed.

This SDT reviewed information on the CIP 005 SAR presented by Scott Mix of NERC staff. Joe Bucciero reported that the NISTIR report released for internal review by NIST.

The Vice Chair and Chair introduced the concept of lunch briefings on key issues or efforts that have been discussed or requested by Team members. They noted that a "forensics" lunch and learn presented by SERT originally planned for this meeting will be scheduled for the Chicago meeting. At this Pittsburgh meeting three sessions were organized and presented:

1. Standard Format Concepts- Proposed New Approach to Scoping Controls Presentation - John Von Boxtel on Tuesday

2. A joint meeting with Darren Highfill and the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) Team meeting at SERT on Wednesday.
3. Substation Networks Presentation- John Varnell

The Chair summarized the SDT agreement reached on the July 2 teleconference to finish CIP 002-4 and ballot it and submit to FERC by the end of the year mean that the Team needs to finish CIP 002-4 by August in Chicago so that NERC staff can review and then the Team will refine and adopt it at the September using initial results of industry survey. The Team will continue working but will have to adjust the CIP 010 and 011 schedule for the industry review and response to after the completion of the CIP 002-4. The SDT explored working simultaneously and separately on survey and CIP-002-4 vs. releasing both at same time. At the conclusion of the schedule and survey discussion on Tuesday, the Chair asked Howard Gugel to develop and present some schedule options for the SDT to consider on Thursday. On Thursday afternoon Howard Gugel reviewed and the SDT conducted two straw polls on the following two options:

Option 1 – Release 002-4 after survey results, provide two days for the SDT to analyze survey results before approving for NERC staff review and send to Standards Committee for approval – only one ballot with possible re-circulation ballot for 10 days. (***Acceptable: 12 Not Acceptable: 0 Abstain: 4)***

Option 2 – Approve 002-4 and all related documents by end of July to post by August 6, release 002-4 concurrently with survey and have a 45 informal comment period without ballot, refine based on comments and another 30 day period leading to the ballot. (***Acceptable: 8 Not Acceptable: 5 Abstain: 3)***

Howard Gugel, NERC staff, outlined the NERC effort draft and conduct an Industry Survey on information that the SDT could utilize in the CIP 002-4 drafting effort. He reviewed the schedule which required industry comments on the draft, BOT approval of the survey and NERC conducting the survey in August with the results due back on September 7, which would be during the SDT's meeting in Winnipeg. The SDT discussed the survey covering the following areas:

- Mandatory information request.
- Justification for Thresholds.
- Focus on Completing CIP 002-4 first.
- Industry Ability to Respond.
- NERC Survey vs. SDT Survey.

The facilitator summarized the conversation noting Team concerns over: the "mandatory" nature of the request, the appearance that the request coming from the team and not NERC; concerns and assurances about how will information be used by NERC; and balancing whether there is any way to accelerate the survey process to have results in time to review in September, yet enough time to respond accurately if "mandatory."

The Chair noted that NERC has already posted a survey document for comment and date for responses to the draft survey cannot be changed. Thirty days for industry response seems to be minimum time we can allow for response to the survey. At the conclusion of the discussed the following motion was adopted:

- The SDT requests that NERC modify the survey language and transmittal letter to state that NERC is requesting the survey and correct the reference that states that the CSO706 SDT drafting team requested the survey. ***(18, in favor, 1 opposed)***

Following the motion, Howard Gugel presented draft survey revisions to the SDT consistent with the motion to address the concerns. On Friday, Howard Gugel asked for SDT feedback on the survey for the following concept regarding "at-large" generation facilities: "Generation Units as CAs that are at-large facilities (i.e. plants whose combined output is greater than the contingency reserve). CCA to be narrowly defined as the shared systems (requires changes to R2)." ***Members favoring concept: 10; oppose 0; abstain 1***

The Team reviewed and discussed a draft CIP 002-4 objective statement drawn from materials provided at the July 2 conference call meeting and suggested taking a few minutes to be sure the SDT agrees on the objective or outcomes we are hoping to produce with the development of CIP 002-4.

John Lim then presented the CIP 002-4 strawman for the SDT's consideration and input. He walked the SDT through the sections of the draft. The CIP 010 sub-team worked on producing this initial draft. The sub-team started with CIP 002-3 and developed a redline of proposed changes. The SDT discussed the draft CIP 002-4purpose statement including whether functions will be referenced.

4.3 exemption from 002-4 and Facilities

Straw Poll In favor removing 4.2? 15 members favor of removal of 4.2, 3 opposed. (83% support)

Requirements

Straw Poll on R2 examples

- How many favor including a list of functions as attachment – *5 in favor*
- How many favor the original R2 with examples? *6 in favor.*
- How many favor the original R2 without examples? *12 in Favor.*

Motion: to remove examples and keep remaining language R2 in first paragraph 14 in favor, 4 opposed. (Passes 78%)

Motion: The SDT objective for CIP 002-4 is to leverage the work already completed by the SDT for CIP 010 in developing a revised CIP 002-4 version that is narrowly scoped to identify

the Critical Assets in the Bulk Electric System through the use of bright line criteria as currently under development in CIP 010. 15 in favor; 3 opposed. Passes (83%)

The SDT reviewed and discussed and polled the proposed revisions to Attachment #1. The following are the Straw Poll results:

- Support for dropping 1.1: 15 in favor; 3 opposed. (83%)
- Support for Revised 1.2 language (a-d). Support for – Support 0 Oppose 19
- Support proposed changes to 1.3 - 13 oppose 0 support ; abstain 7
- Support section 1.4 as changed: 14 support; 5 oppose (74%)
- Support 1.5 as revised – 18 in favor 0 opposed, 1 abstain (100%)
- Support 1.6 as revised – 19 in favor 0 opposed (100%)
- Support including 1.7: 18 in favor; 0 oppose; 1 abstain. (100%)
- Substitute in 345kV –5 in favor; 14 oppose. (26%)
- Support 1.9 original language with FACTS and IROLs: Support 12; Oppose 0; Abstain 6 (100%)
- Delete the second sentence in 1.9 –14 in favor: 0 oppose: abstain 3 (100%)
- Proposal to use “control center” – Support 17, Oppose 2. (89%)
- Proposed language without limits for 1.14-1.16: 10 in support; Opposed 10 (50%)
- Support for: “Any control center or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions. Support 13; Oppose 1; Abstain 8 (93%)
- Support for: “Any control center or systems and backup control center or systems performing RC functions.” 17 in support; 0 Opposed Abstain: 1 (100%)
- Support for Approach: Appropriate to incorporate bright line criteria from attachment 1 into the risk based methodology. Support 8 Oppose 12 (40%)
- Support for Thresholds on 1.18- 9 in Favor; 8 Oppose ; 1 Abstain (53%)
- Support for Thresholds on 1.19 10 in Favor; 8 Oppose ; 1 Abstain (56%)
- Support for Thresholds on 1.20. -12 in Favor; 6 Oppose; 1 Abstain (67%)
- Support for taking out distribution provider in 1.15: Support 14; Oppose 1; Abstain 1 (93%)
- Support for Wording in 1.14 and 1.15 from 002-3 R1.25 – “System and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.” Support 14; oppose 0 (100%)

On Friday morning the Vice Chair asked each Sub-team lead to give a report on progress since the Sacramento meeting. He suggested that as a minimum, each sub-team should complete its summary of industry informal comments received as well as the Dallas workshop input so a response document can be developed and be prepared for posting. Each of the following Sub-teams presented updates:

1. Systems Security and Boundary Protection (Jay Cribb, Lead)
2. Recovery Management Scott Rosenberger (Lead)
3. Personnel and Physical Security Doug Johnson (Lead),
4. Change Management, System Lifecycle, Information Protection, Maintenance, and Governance. Dave Revill (Lead)\
5. Access Control Sharon Edwards (Lead)
6. Implementation Plan Sub-Team Scott Mix (Lead)

The Vice Chair thanked the sub-teams for the significant work done by sub-teams despite the political sideshow. He noted he had underestimated when the SDT could get back to CIP 010 and CIP 011which may not be until December. Many in industry will want to know what was said and done at the Dallas workshop as well as the industry's informal comments. We need to decide soon how we want to address and respond to those in the future, but for now we need some closure on summarizing the comments we have received. WE may need a conference call or a webinar to explain why we are moving 002-4 and putting the 010 and 011 on hold. He urged each sub team to hold at least another call in order to create a response summary to industry comment by the Chicago meeting.

The SDT then conducted an initial discussion of CIP 010 and 011 Schedule. The Vice Chair noted the Team will review and adopt a proposed schedule in Chicago to send to the Standards Committee.

Phil Huff noted the 002-4 team will continue working. He discussed developing a revised schedule with 3 full days of meeting after September. Finally, the Vice Chair, on behalf of the SDT, thanked Sam Merrill and the CERT for their excellent hosting and facilities. He noted Doug Johnson will be our host in Chicago in August and urged members to register for the session.

Meeting adjourned at 11:30 a.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

24TH MEETING SUMMARY
Cyber Security Order 706 SDT- Project 2008-06
July 13-16, 2010
CERT Software Engineering Institute, Carnegie Mellon University
Pittsburgh PA

I. AGENDA REVIEW, WORKPLAN, SCHEDULE AND REVIEW OF NERC SURVEY

A. Agenda Review

On Tuesday morning, the Chair, John Lim and Vice Chair Phil Huff welcomed the members to the SDT's 24th meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host, Sam Merrill a participant in the SDT sub-team process, welcomed everyone to Pittsburgh and Carnegie Mellon University and the meeting facilities and he reviewed the history and role of SEI in cyber security and covered logistics.

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

The Chair noted that the Team had met by conference call/ready talk three times since the Sacramento meeting to review and adopt a revised schedule to produce, ballot and send on to FERC a narrowly framed CIP 002-4 by the end of 2010. He also pointed out that the draft agenda sent out the week before has been revised based on member feedback so that the Team will be meeting together in a plenary format until at least Thursday. He then reviewed the following proposed meeting objectives:

- To review the CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4
- To explore and clarify the Work Plan and Schedule for completing CIP-010 & 011
- To review, clarify and refine the strawman CIP-002-4 standard proposal
- To receive presentations on forensics, sub-station networks and advanced persistent threats
- To convene sub-teams to review the sub-team responses to Industry comments and proposed changes to CIP-010 and 011
- To provide SDT guidance so sub-teams can make further refinements to CIP 002-4, 010 & 011

- To agree on next steps and assignments

The Vice Chair, Phil Huff noted the inclusion of "lunch and learn" sessions that are intended to present helpful additional information and briefings as requested by the Team. Bob Jones, facilitator, reviewed the proposed timed meeting agenda *(See Appendix #1*). The Team agreed to proceed with the agenda and on Thursday morning the SDT approved without objection the meeting summary for the June 8-11, 2010 SDT session in Sacramento, California.

B. SDT Consensus Procedures

The SDT were sent, as part of the agenda packet, some changes being suggested by the Chair and Vice Chair. (See Appendix #). Phil noted the challenge of maintaining a quorum in meetings when the Team has grown to 26 members. The current rule requires at least 2/3s of the members (18) present to establish a quorum. The proposal is to ask standards committee to allow 50% +1 rule for the SDT which would mean we would need 14 members present to establish a quorum. Phil Huff moved to and John Lim seconded the motion to change the quorum rule.

Discussion Comments

- Have we ever not had quorum at in person meeting? (Yes) Problem is with decisions on conference calls that we cannot participate on. May not be aware of the meeting and decisions will be made without members knowledge.
- Two conference call meetings in June to discuss and adopt a revised schedule had to be rescheduled due to lack of quorum.
- The is a quorum, not decision rule
- Could have two votes on two days and have different results?
- Why has the SDT gotten larger? A: Two new members were appointed by the Standards Committee to help the SDT with nuclear issues.
- Did not know that. Not happy about increasing size of group – why do we schedule decisions for Friday mornings instead of Tuesdays – Is this a scheduling issue?
- Concerned that we need to look at both rules together. So if we drop to 50% +1 quorum and down to 2/3's to make a decision, then it would be possible to make a decision with 2/3 or 10 of 14 or can make decisions with only 38% of the members.
- May also need to address issue of members who do not regularly participate but require a larger quorum.
- Not all of the SDT's business, considering the amount of work we need to do, can be done in person and requires phone review and votes. Yes, we need to address the issue of regular participation too – may need rules about participation in person and

by phone. Ready talk counts as participation to in-person meetings – when members agreed to join the SDT there was an expectation you could meet the obligation to participate. It would help for member to notify leaders if you can not make calls. When we send a notice of a call, the assumption is everyone can participate.

- We do try to participate on calls and we do have a real jobs. I commit to make the whole meeting as schedules. There should be no excuse to leave early. Friday votes may be necessary to follow on discussion and review at in person meetings – have to make the effort to be here, that is the commitment .
- I think that is a good point – commitment is to be available, even if team meets more often and longer than most – this team does not determine the standard, the ballot body does – you need to get something to the ballot body.
- Suggest that if the expectation is for more SDT conference calls, then we should schedule ahead of time on regular basis in order to allow us to reserve time in our schedule – one week notice is not enough time to set aside time for calls.
- Is the 2/3's vote for approval 2/3's of those present where there is a quorum? Yes.
- Need to understand in order to make judgment on quorum. It would mean that less than half the team could make decisions.
- Most standards teams are smaller and do not even have votes.
- This is a new subject, thus the larger team and more difficulty in making decisions

A straw poll was taken of those members in favor of changing quorum: 4 in favor: 16 opposed. (20%)

Following the straw poll the motion was withdrawn.

The second proposal was for changing 75% decision rule to 2/3's. Phil Huff made the motion and John Lim seconded.

Member Discussion

- This change might assist the SDT in making decisions more quickly and moving team forward and it follows the 2/3 quorum.
- 2/3 is the standards process default – team used 75% when it was smaller and to achieve higher approval level. This has proven difficult with the quorum at 2/3 (i.e. 18 members) 75% may be even more difficult to achieve and move the team forward.
- We need to be able to move forward with certainty. This is a brand new area, and in order to effectively convince industry we need to be sure team is fully on board. On any vote we have had, we have 1/3 on each side with the middle third going one way or the other – we need a substantial margin to ensure even members disagreeing on

particular issues can support decision on the package once made. WE need to hold ourselves to a higher level

- Do we need a quorum at time of the vote? A: yes. SM – quorum must be present at time of vote according to NERC's legal counsel.
- Need to be able to bring some of the dissenting third on board into the decision if we then want to sell it to the industry. In the end we have to do a better job of selling issue to the industry and that starts with building consensus in the room.
- We also have to be willing to compromise and some individuals in this room have found it hard to compromise – taking hard positions and refuse to move – too many on the team

Motion: To change the 2/3 decision voting rule for the SDT to 2/3's from the current ¾ 's (75%).

17 in favor 3 opposed Passes (85%)

Comments after the Vote

- We need to promote member participation and schedule votes well in advance – need to bring the dissenting side along as much as possible – need to work together, collaborate on decisions
- It is easier to schedule early and cancel than to schedule late.
- We will try to schedule votes ahead of time as much as possible – members need to reply if they cannot make it so we can have an idea if we will have quorum – if you do not respond, assume you will be able to make it.
- Is a proxy vote or vote *in-abstentia* possible? A: not allowed under NERC's standards rules.
- May not have an hour for long discussion but can jump on for quick review and vote in 5 to 10 minutes – also need subject of the vote to determine importance of participation.
- We will clarify if a call involves a vote and what subject of the vote will be.
- Can we use an on-line voting tool that allows us to read it and cast vote over a period of time? The SDT approved an email voting provision but it is very limited in its use.
- We also need to allocate enough time for calls in which votes will be taken.
- Set regular schedule of time blocks for possible calls such as every two weeks.
- Voting in the interim between meetings has been used twice due to time and schedules – also, note the last month was sloppy due to requests from the Standards Committee – not a good precedent – hopefully used only in emergencies – blocking off time is a good idea, but use only if needed.
- The consensus process provides that the SDT strive first for unanimous agreement based on thorough discussion but that depends on willingness of some not to oppose after thorough vetting of issues and concerns – have to be willing to listen to others as well as argue your own point – broader effort to get quality product from the collective knowledge you bring to the table.

C. Related Cyber Initiatives

1. CIP 005 SAR.

- Scott Mix provided an update on urgent action process for reviewing CIP 5 - SAR is done and the standard is 80% complete – deals with support and maintenance from vendors and the devices used for remote access – wholly impractical to have critical assets located at vendors. Jim Brenton noted he was involved and it was a good team. They are clarifying terms including the use of laptops for system maintenance and vendor access – look at advisory and it sets out the valid reasons for the vendor access and need for control and oversight of the laptops.

Member Discussion

- How can I get involved?
- What is the relationship between the CAN information, Jim's team, and our effort? A: CAN and urgent action process relationship? None – for this team, need to be sure later work on 011 matches up with work done by the CAN and Jim's team.
- Do this replace this teams work? –The process is very unclear
- No, but need to be sure they match up
- Almost all support can access the system and test operations – the CAN missed the mark, puts the grid at risk by limiting our efforts to make process and access more efficient – reduces reliability rather than enhances
- Urgent action is a new version? When is it due out? May cause confusion
- All hits about the same time
- Seems like it will slide in well with the draft maintenance section in 011
- Six wall perimeter and how you handle it – careful if we are changing ESP's
- Reviewed the people working on the urgent action team

2. NISTIR Report

Joe Bucciero reported that the NISTIR report released for internal review by NIST – three volumes – to be released soon to outside review – will not go through a FERC process before release to industry and is not subject to formal FERC approval.

Member Comments

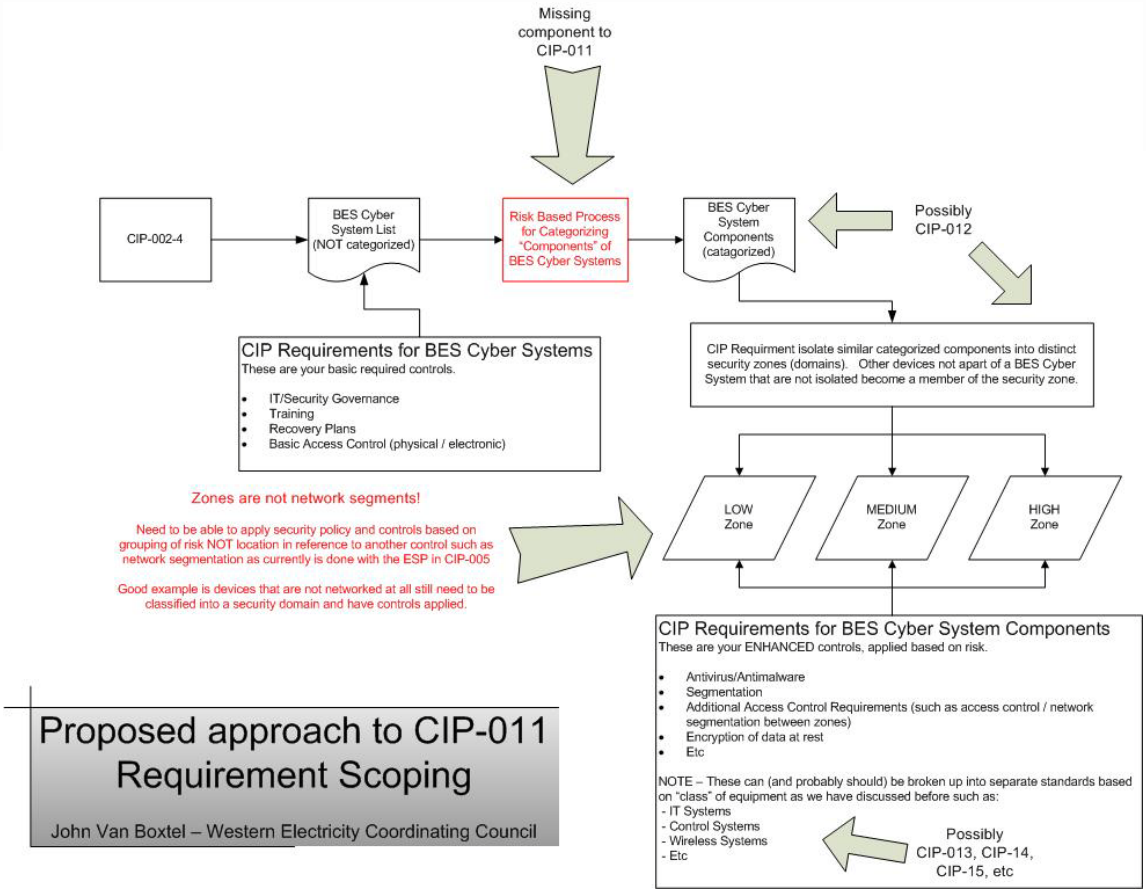
- FERC is providing input if not formal approval
- CCI guidelines completed and now official
- Cyber security group formed by NASBE too – still high level at this point
- Has anyone discussed Senator Collins Bill? It includes a requirement to report cyber incidents to new Homeland Security director position.

D. Lunch and Learn Sessions

The Vice Chair and Chair introduced the concept of lunch briefings on key issues or efforts that have been discussed or requested by Team members. They noted that a "forensics" lunch and learn presented by SERT originally planned for this meeting will be scheduled for the Chicago meeting. At this Pittsburgh meeting three sessions were organized and presented.

1. Standard Format Concepts- Proposed New Approach to Scoping Controls Presentation - John Von Boxtel

John Van Boxtel presented a proposed different format approach to scoping and tailoring controls to risk. This would be an approach that would leverage the work on CIP-010 while solving some of the problems with trying to apply controls only based on the impact level of BES Cyber Systems. The main proposed difference is to apply a base level of controls at a BES Cyber System Level and to apply additional controls to the BES Cyber System Components based on grouping into different security zones based on risk for the SDT to consider. During and following the presentation the SDT informally discussed some of the ideas presented.



Member Discussion

- Changing words to zone or segment is not effective – now we have high, medium and low – should have different boundaries – if not connected then just a physical boundary.
- You can have protection around h-m-l and have further system segregation for high assets
- If you have one high connected to low – the attack will come through the low to get to the high.
- We need to break things up based on risk, not as part of systems.
- Separating those that are at risk from those that are not is the "crux of the biscuit" (Frank Zappa – apostrophe album) Further segmentation is the concern. "Domain" means different things in different contexts.
- What about calling them "zones"?
- How do you segment zones
- Initial requirement in 011, then additional requirements in subsequent standards to further layer on additional controls for specific zones.

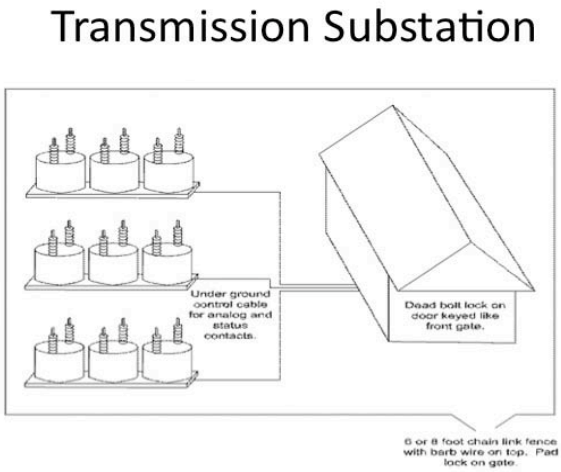
- How would you determine high-medium-low?
- Still have to establish the criteria.
- Is this biased toward the controller? Problematic if bringing in broader ring of corporate assets.
- This may be the "three by three" matrix creeping back – zone classifications come out of that matrix.
- This is similar but a little more broken out.
- The red box pulls the multiple matrix back in and we do not have time or understanding to pull that together.
- This is a separate standard from 010
- The multiple matrix was only in the concept paper and the industry gave strong feed back not to do that because it was too complicated.
- Might be more receptive if you give industry their own risk based methodology for figuring out the h-m-l –
- Problem with the "red" box is that it moved away from "acceptance of risk" to meet FERC concerns – if identify as critical then you have to be prescriptive.
- Also, how do multiple zones work within one interconnected system?
- It will depend on how they are connected to determine the vulnerability of a component – two separate sets of risk assessment.
- This might work with IT but not in the power industry.
- This is where the smart grid is headed.
- This will give too much leeway to a few to screw it up for the rest of the industry – need to universally apply standards to be fair. Could create a competitive disadvantage for fully identifying critical assets.
- This works if the team can come up with something reasonable for the red box.
- Previous teams wrestled with this issue. You can use categories, classes or zones, but Mike Peters at FERC consistently says that everything needs something – you have the production and the distribution – baseline is and ought to be different for a control center and a substation – give thought to differences in the physical location. We have been thinking about big, medium and little iron. The Team should think more about the connection to the system.
- Zones allow for baseline for everything and additional protection for a control center – have to address the issue or will be wasting time on 011.
- Taking something from routable to serial should not be considered gaming the system – instead it is a business decision.

- Is the SDT getting away from 706 – take what is in the order and fix 003-009. (*participant)*
- 4.2.1? FERC asked for clarification – should cabling be exempt if within the physical boundary (*participant)*
- Use base level of protection on all assets and a cyber risk assessment above and beyond the base.
- Also tired of hearing about gaming – it is business decisions – we do not have a well defined problem statement – clarifying what are we trying to accomplish will be key to project management.

2. **A joint meeting with the ASAP-SG Architecture Team meeting at SERT on Wednesday.**
   Darren Highfill and the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) Team met with at SERT with the SDT and discussed possible opportunities for coordination.

3. **Substation Networks Presentation- John Varnell**

John Varnell presented information on Sub-station Networks for the SDT to consider. During and following the presentation the SDT informally discussed some of the ideas presented.



II. CIP 002-4 REVIEW AND REFINEMENT

A. CIP 002-4 Schedule

1. Initial CIP 002-4 Schedule Issues Discussion

The Chair summarized the SDT agreement reached on the July 2 teleconference to finish CIP 002-4 and ballot it and submit to FERC by the end of the year mean that the Team needs to finish CIP 002-4 by August in Chicago so that NERC staff can review and then the Team will refine and adopt it at the September using initial results of industry survey. The Team will continue working but will have to adjust the CIP 010 and 011 schedule for the industry review and response to after the completion of the CIP 002-4.

Member Comments

- Results will be essential to setting metrics – however there is a scheduling disconnect that will not allow the Team to review, analyze and incorporate the learning from the survey results into CIP 002-4 that same week.
- The facilitator noted that the Team had tried to change SDT meeting to the following week but that would conflict with CIPSE meeting which a number of Team members and NERC staff directly participate in.
- Can we cut some red tape and streamline the survey process? Looked carefully at this but there is very little flexibility in the notice times etc.
- Critical path for the SDT is through the survey. We need to find a way to accelerate the survey to get the info back sooner – no one looking at it yet because the date is too far off in the queue of work. NERC President, Gerry Cauley, may be the only one who can light a fire and get it done
- We need a schedule we can all live with. Concerned about the confusion this might create in the industry. Looking at the overall 010 and 011 schedule, it looks like industry voting in February while 002-4 moving through approval with FERC?
- The schedule only provides for 2 CIP 002-4 ballots with the 2nd in December.
- The Motion adopted on July 2 by the SDT call does not include balloting beyond 002-4. The CIP 010 and 011revised schedule has not been discussed and approved by team yet.
- A draft of the survey was briefly reviewed by Howard Gugel with the SDT at the July 2 conference call meeting on schedule. There is an appendix of the draft in the July 2 meeting summary.
- The SDT agreement was to complete CIP 002-4 without impacting the CIP 010 and 011 effort. However that is not realistic. We need to continue to work on these simultaneously, however we should focus on completing 002-4 first.

- Is the comment period required under the NERC rules of procedure? Yes, and it is being expedited.
- **Working Simultaneously and Separately on Survey and CIP-002-4 vs. Releasing both at same time.**
- Why can't the survey be part of the info requested during the posting of CIP 002-4? Try to fold into the comment period?
- NERC is under pressure to get numbers to share for Congress.
- NERC is proposing not folding the two together but rather conducting simultaneously and separately with CIP 002-4 for comment at same time the mandatory survey request is out.
- What about finishing CIP 002-4 complete by end of the Chicago meeting and put out simultaneously with the survey?
- If we try to finish by end of the SDT August meeting and post at same time as the survey, we might buy some time for a third ballot but we would have to complete our work at this meeting so NERC staff could review between now and Chicago.
- Are we severely underestimating amount of work needed for 002-4? The Team should consider dividing up to work on 002-4 and the rest of the Team could continue to work on 010 and 011. Bringing this up now because it impacts any proposed schedule.
- The NERC survey is intended to help the Team to understand if we have the line for heavy/medium drawn in the right place –Question 1 and 2 are quick, 3 may take a little more time – if compress it, industry will express concerns about the validity of result.

2. Review and Testing Consensus on CIP 002-4 Schedule Options

At the conclusion of the schedule and survey discussion on Tuesday, the Chair asked Howard Gugel to develop some schedule options for the SDT to consider on Thursday.

a. Option 1- Conduct Survey in August, Post CIP 002-4 in September

On Thursday afternoon Howard Gugel reviewed with the SDT the Option 1 schedule which called for release of the NERC survey in August, the SDT analyzing survey results at their September meeting before approving for NERC staff review CIP 002-4 and send to Standards Committee for approval. It would provide for only one ballot with possible re-circulation ballot.

Member Comments

- Line 53 – what criteria will be posted in the survey?

- Date actual survey will go out – include the teams output – may be additional data points that NERC staff will include such as 1.1 – not painted as a request from the team, only from NERC – very quick turn around – may add an arbitrary line for "medium" to get additional level of data.
- May cut "high" in half for "medium" as a data point.
- Line 56 – challenging to get results and make decisions by that next Friday
- Two days is for team to analyze – survey closes in thirty days during the SDT Winnipeg meeting.
- Survey finalized by 7/26? Good chance "high" as we have it will not identify enough – think in Chicago about "what if" scenario responses to possible survey results – wait until September and results in hand may be difficult.
- This approach takes away from getting other work done.
- May need to organize discussion to test potential responses.
- May be better to let a sub group of 2-3 create straw man without putting too much full team time into speculative responses.
- Trying to back everything into same time period – May need to schedule a team call for the Sept. 15th? Same day as CIPC meeting.
- Will NERC put in request for information on nuclear even if not in the current version? A: Yes.
- Will gain assets, stay the same or will lose assets – industry fears impact of increased number and cost impact and decrease on political optics - any space for narrative responses we have to respond to? A: No, data only.
- Comment period is on now for survey structure – this schedule is very tight.
- How can we work on this, on 010 and 011 and our real jobs too?
- NERC staff will prepare draft responses to the first posting of 002-4 as starting points for the team to work on.
- Will we work on the other documents related to 002-4 in Chicago in August – comment form, VSLs, etc.?
- Might be of value for each of us to fill out survey as a subset of the survey and use as an example to think about responses at the Chicago August SDT meeting.
- What about the implementation plan for 002-4? A: 24 months as planned for 002-3.
- We should consider splitting into separate teams to make progress on 010-011 and the 002-4 in the time given
- Even if initially review, we still need full team review for approval and adoption.

- Should we consider going to the Standards Committee to split the team into two separate teams to work on the two tracks?
- Schedule needs to reflect the implementation plan and other related documents for 002-4 and factor in the time needed.
- We will need to focus full group time to review and discuss – small sub group could bring a product forward.
- It will be folly to think much progress will be made on 010-011 until end of the year and work on 002-4 completed – given a new directive.

Straw Poll
Option 1 – Release 002-4 after survey results, provide two days for the SDT to analyze survey results before approving for NERC staff review and send to Standards Committee for approval – only one ballot with possible re-circulation ballot for 10 days.

Acceptable: 12 ***Not Acceptable: 0*** ***Abstain: 4***

b. Option 2: Post CIP 002-4 along with Survey

Howard Gugel reviewed with the SDT the Option 2 schedule which would allow for two comment periods, issuing the first version of 002-4 along with the survey. The SDT will have to respond to two comment periods and need an approval by end of July for CIP 002-4 – not a ballot – but includes implementation plan.

Member Comments
- May get the same result from option 1 by putting content into the survey.
- The thought here is that people prepare comments along with survey and gives team two shots at explaining rationale – providing the pros and cons to both approaches.
- Which option offers most time to evaluate data – only two days in the first option and seven days in option two?
- Favor second option – still don't see us making progress on 010-011 until end of the year with either option.
- Hopefully the survey will inform our understanding and rationale.
- The survey will inform the second posting in this option
- The work products due with posting means the SDT will have only two weeks time to review and develop the implementation plan under this option
- With option 2, how much harder will it be to make changes based on survey input?

- May be easier with two comment periods in option 2. The first comment period does not include a ballot.
- Explanation of the criteria may not be enough – balance realities of what has to happen with what industry may say if there is a big increase in assets identified.
- In terms of the implementation plan, if you don't have to recreate critical asset plan then that will greatly reduces the amount of work
- The first option allows us to make changes and justify using the survey results.
- May be a lot of association pressure to pass whatever version we put out regardless of grousing.
- An implementation plan requiring changes would not be justified at this point. It should be a relatively simple plan – probably able to prepare in three days.
- CIP 003-009 changes are just conforming? Yes
- Yes, except for the other group on CIP 005 which may only confuse the industry more
- Survey going out independently might mean the data is less skewed.
- Delivery of CIP 002-4 by the end of July is the major problem with Option 2
- Possible exception for additional documents with the posting? A: probably not.
- Much of the comments last time related to the lack of related documentation – people want to know the rationales.

Straw Poll

Option 2 – Approve 002-4 and all related documents by end of July to post by August 6, release 002-4 concurrently with survey and have a 45 informal comment period without ballot, refine based on comments and another 30 day period leading to the ballot.

Acceptable: 8 **Not Acceptable: 5** **Abstain: 3**

B. NERC Industry Survey and CIP 002-4

Howard Gugel, NERC staff, outlined the NERC effort draft and conduct an Industry Survey on information that the SDT could utilize in the CIP 002-4 drafting effort. He reviewed the schedule which required industry comments on the draft, BOT approval of the survey and NERC conducting the survey in August with the results due back on September 7, which would be during the SDT's meeting in Winnipeg.

Member Comments on Survey

Mandatory information request.

- Is this a mandatory request? Yes, industry must respond. However there is a statement that the data will not be used to monitor compliance.
- NERC is using a "mandatory" request to insure timely responses that can be used by the SDT. There was a request at the Dallas workshop for a voluntary response which was met with total silence. However the mandatory 1600 process brings with it a slower bureaucratic process.
- People concerned are at one level above those who have to respond – yes, you probably need to go mandatory.
- It would be possible, but perhaps not advisable, to post CIP 002-4 during the survey, but we cannot delay the survey to look at final version and meet the December deadline. We would have a scheduling nightmare, the proposed schedule is the only way to physically meet the deadline.
- NERC realizes Congress and Senate up for reelection and under pressure to do something – Gerry Cauley needs hard numbers to fend off pressure. I misunderstood and told my folks it would not be mandatory and would be anonymous.
- Of mandatory then it may raise flags of concern in the industry that it will be used against us.
- Uneasy feeling that this is about FERC and Congress asking if this is enough critical assets – what are we going to do with the data, nothing – what if the the former says it is not enough assets?
- Comfortable with an informal survey but mandatory response will put team in position we do not want to be – this may mean the list will have to be the same as the final list we will be requiring – if it is not the same, what happens to the company – if numbers don't match, companies may find themselves in hot water? A: The survey instructions say the survey is to only inform the team and guide development of the standard. We are looking for a reasonable response, not an exhaustive one. The survey also states how the data will be used, and that is will not be used for any future compliance action or monitoring.
- This will still be seen by industry as a legal requirement.

Justification for Thresholds.

- 002-4 uses same bright line criteria, sort of, as 010 – told we need to provide clear basis for bright line – industry feels they are arbitrary – the questionnaire just moves the arbitrary line – we tweak the lines to get the number we or someone else wants? Difficult to establish the basis for the threshold, boat load of work
- The industry perceives little difference between team and NERC. Why put the times together? Industry is confused why going back to 002-4 from 010 – conflicting message, survey just adds to the confusion.

- Concerned that we have roughly same set of criteria on three different development tracks – 002-4, 010 and survey – survey may not be in sync with team's work on 002-4?
- The team must provide comment saying this is what we want to include in the survey
- NERC and team are not seen as the same in the industry – industry understands the difference – also, is NERC management going to push back if we change 002-4? That is why it is important to ask industry based on the changes to 002-4
- Still not really getting a bright line
- People appear more concerned about the political perception of "high" than actual number
- We will not have any more assets identified than before?
- Some confusion in industry but to try and resolve the confusion may cause more confusion through industry as a whole.
- Similar concerns are that we are not resolving the correct issue and just stopping to identify assets, not identifying the correct critical assets – the survey doesn't get at the latter.

Focus on Completing CIP 002-4 first.

- Need to focus on getting 002-4 done first
- Depending on when schedule is needed for the 010 and 011 – we need to push that off and focus on getting 002-4 done.
- How much time do we spend on 010 and 011 sub team reports versus focusing on 002-4?
- We have three days, we could get 002-4 done by Friday – just proposing a few days delay on 010 and 011?

SDT to Summarize CIP 010 & 011 Informal Comments and Workshop Input in August.

- We should not suspend 010 work. Indeed the work on 002-4 should inform 010
- We had an informal comment period and teams have addressed those comments for 010 and 011 – we should not stop, but provide comments – have to balance tasks
- Need to get 002-4 out – also need a schedule that reflects reality about getting 010 and 011 out.
- Since there was not unanimity among the SDT about going forward with 002-4. Consider the possibility of splitting our resources to make progress on both tracks –

also allows those who don't support 002-4 approach to distance themselves from that process.

Industry Ability to Respond.

- Will industry be able to provide this information in a such a short interval? The survey was designed to be relatively straightforward to complete with existing CIP data.
- The chair noted that the Team will have to wait and see results before we can evaluate – will do what we can in September and hold additional calls, if needed, to finish work.

NERC Survey vs. SDT Survey.

- This language needs to be clarified that request is from NERC, not from this Team.
- Howard Gugel agreed to take the SDT's suggestion into account in finalizing the survey.
- The team did not ask for the survey, do not present that way – request is from NERC – don't like the politics affecting technical questions, but that is the reality – there is no identified number of critical assets just a politic perception – not thrilled with approach but that is what we have to do to get the job done.
- Seems to be too much red tape here – team had nothing to do with this and should not be presented as requesting the information
- Appears NERC is asking for a lot of data in just two weeks? A: Only asking for comment on the survey in two weeks before getting BOT sign off, then there will be 30 days.
- Even thirty days requires legal and management review – question why we are requesting – remove our name and say NERC wants to know.

The facilitator summarized the conversation noting Team concerns over: the "mandatory" nature of the request, the appearance that the request coming from the team and not NERC; concerns and assurances about how will information be used by NERC; and balancing whether there is any way to accelerate the survey process to have results in time to review in September, yet enough time to respond accurately if "mandatory." The Chair noted that NERC has already posted a survey document for comment and date for responses to the draft survey cannot be changed. Thirty days for industry response seems to be minimum time we can allow for response to the survey. NERC should look to whether it might be possible to shave a week to post survey sooner than the August 6th date. Request NERC look at end of comment period and posting of the survey. Howard Gugel noted that NERC staff need time to analyze and comment on industry comments

and make possible changes to survey and produce a recommendation for review by the Board of Trustees as urgent action on August 5, in only nine days.

After additional facilitated discussion which highlighted that the SDT could use any resulting information to inform and modify their standards drafting going forward, Sharon Edwards made and Jim Brenton seconded the following motion:

- **The SDT requests that NERC modify the survey language and transmittal letter to state that NERC is requesting the survey and correct the reference that states that the CSO706 SDT drafting team requested the survey.**

Having confirmed a quorum, the Team adopted this statement *(18, in favor, 1 opposed)*

Following the motion, Howard Gugel presented draft survey revisions to the SDT to address the concerns. Howard noted that he had replaced "team" with "NERC" – also bolded the language that data not used as basis for determining compliance.

Member Comments

- What does "currently enforceable" mean? Could be used for 002-4? Add the phrase "and any future standards"? By saying one and not the other, it leaves open the question.
- NERC would be using the data cumulatively to determine compliance in the future
- Does the data assists and validate the standards, not compliance? Yes. This is not meant to apply to any individual
- NERC should modify to include that clarification.
- Not used for compliance of individual entity but cumulative for determining compliance standard.
- Worried it flags issues for auditors to look at going forward – "currently" cannot be used here – put in the specific language.
- Regions need to clarify the auditors cannot use the information for future audits
- Roger Lampila noted the information is only going to NERC not the regions. I would hope you would say no if the region came and asked for the info. That list for the survey should have no basis for the audit.
- Clarify that it won't be used for compliance and you will publish a cumulative compilation, not individual data.
- In addition, note that Section 1600 mandatory request provisions do not apply to compliance actions. This should be put that into the statement

On Friday, Howard Gugel asked for SDT feedback on the survey for a concept regarding "at-large" generation facilities. He noted the need to know what attachment will look like for CIP 002-4 since the survey will key off of that. The SDT discussed the need to draw lines for control centers and the characterization of high and medium- "darts", noting that we should try to find points that industry can easily fill out and that also helps the team draw some lines in CIP 002-4. He then asked the SDT to give him feedback on the following:

Concept: Generation Units as CAs that are at-large facilities (i.e. plants whose combined output is greater than the contingency reserve). CCA to be narrowly defined as the shared systems (requires changes to R2)

Discussion of Concept

- Targeting reliability factor
- Do assessment for CA then go back to CCA?
- Looking at aggregate impact
- Before it was the sum of the reserve
- Attempting to use the balloted language
- Generator would know if they exceed the minimum requirement of shared system
- Headed in the right direction – but point out "plant" is ill defined term much like difficulty we have had in defining control center.

Favor concept: support 10; oppose 0; abstain 1

C. Discussion of CIP 002-4 Overall Objectives

The Team reviewed and discussed the draft CIP 002-4 objective statement. Bob Jones reviewed the statement which was drawn from materials provided at the July 2 conference call meeting and suggested taking a few minutes to be sure the SDT agrees on the objective or outcomes we are hoping to produce with the development of CIP 002-4. The strikethrough and underlined reflect the discussion comments below but not effort was made to test for SDT support for the statement.

> ~~"Both NERC and the Standards Committee, with concurrence from major stakeholders and trade associations, believe there is a need for the SDT to develop a CIP 002-4 consistent with its approach to CIP 010 and 011 in order to demonstrate industry responsiveness with very high stakes in play. The SDT's revised work plan and schedule will provide additional time for the SDT to~~

~~produce a quality product for the next formal posting of a very substantial package of CIP-010 and CIP-011 with associated required documents.~~

The SDT ~~agrees to~~ will work to accomplish the following ~~objectives to~~ in developing a CIP-002-4 in 2010:

1. To provide an incremental step forward towards developing a CIP 010, CIP 011,etc. as new CIP standards for industry review and acceptance in 2011.
2. To leverage the work already completed by the SDT for CIP-010 in developing a revised CIP-002-4 version that is narrowly scoped to ~~more fully~~ identify the Critical Assets in the Bulk Electric System through the use of bright line criteria as currently under development in CIP-010 in place of the risk-based methodology in CIP-002-
3. ~~To ensure that we have covered all of the nuclear facilities and 500kV transmission facilities in the CIP-002-4 bright line definitions.~~
4. To meet the goal for a successful industry standards ballot and filing to FERC of the revised CIP-002-4 before the end of 2010."

Member Comments

- Objective 4? All we can do is put proposal out and respond to comments but we cannot be sure it will get to FERC by December
- Objective #1? Agree that we want to be responsive to industry but question what NERC supports and what the team is doing.
- Not sure the opening it is a true statement – portions of the industry not on board
- Seems disjointed as to the trade associations
- Representatives from trade associations on the July 2 call seemed to suggest they support this support. Allen Mosher addressed the team on this.
- The executive committee of the Standards Committee expressed support for this approach.
- Objective 3 – problem with including nuclear facilities and 500Kv facilities as bright line specifically in the criteria. Suggest deleting here and addressing in CIP 002-4 as appropriate. It might be better to address these in next CIP 010 and 011 and not a bright line assessment.
- It is confusing as to who is speaking at different points in this statement – first part seems to be a call to action from NERC and the 2nd sentence a response of team – may need to clarify into the first paragraph as the call and 2nd paragraph as response.
- Suggest deleting the opening paragraph.
- Concerned with the phrasing "more fully" Suggest removing the phrase – identify critical assets using the bright line criteria.

- What is the purpose of this exercise? How will this statement be used? We are off of our focus if we are dealing with critical cyber assets.
- SDT still needs to clarify what are we trying to protect and from whom with the CIP?
- The point is being sure we have a common basis for this effort moving forward.
- If we want the statement to guide us, we would need more team time refining it. We do not need this for the SDT to move forward on 002-4.
- The facilitator clarified that there is no need to refine and test the acceptability of the statement and it will be reflected in the meeting summary as a set of discussion point.

D. Review of CIP-002-4 Strawman

John Lim presented the CIP 002-4 strawman for the SDT's consideration and input. He walked the SDT through the sections of the draft. The CIP 010 sub-team worked on producing this initial draft. They started with CIP 002-3 and did a redline of changes.

1. Purpose and Appliability

- In the purpose statement, it says we are not changing CIP 003-009. Does that require a separate purpose statement for those and would that cause confusion?
- There is intended to be no changes to the CIP 003-009 requirements
- Are we changing the purpose statement for all of the standards
- Are the changes considered local to 002 or across the standards as we always did before?
- The Sub-team is just conforming changes to 003-009, not changes to the requirements.
- Only substantive changes will be in 002 – let others worry about conforming changes.
- We will have to change version numbering for 003-009 to show conforming changes.
- First word of third paragraph – "business"?
- That was already there in the earlier versions

Functions

- Are functions folded into this? If not, do we need to add something to the end of the sentence? How are we attacking the drafting? not a substance question.

- At the last sub-team's meeting they agreed to remove all reference to functions. Not all members were on and some expressed concerns regarding the treatment of functions
- There are also outstanding issues when we get to applicability if we remove nuclear. The current CIP 003-009- 3 says not applicable to nuclear and to include it would be an applicability change, not just a conforming change.
- Can follow a later schedule for the conforming changes?
- Because we include the nuclear industry we may need to put out for 45 day comment period – can be posted as a package
- We will have to have a detailed technical team meeting to review –SE – the purpose statement has changed – need consistency for applicability
- No one is proposing changing the purpose statements for 003-009 – each will stand on their own with version changes only because of applicability to nuclear – also included in R2 examples of control centers – other things we need to capture and add to the sentence.
- These are not examples – industry wants us to tell them what we need to do – allow industry to do risk based assessment but with clear guidelines, tell them what to put into the risk based assessment – industry would accept that as a slight adjustment and clarification.
- First concern is time – can we make December time if we have to revise whole set of 003-009?
- We are trying to keep within scope to get it to the industry and on to FERC by December. We are not trying to include all of the work in CIP 010 in CIP 002-4.
- We are really trying to tweak 002 and not bring all of the work on CIP 010 into the CIP 002-4
- We will have the purpose statement for 002-4 but new language in the purpose statements in CIP 003-009

Applicability- Distribution provider

- The draft suggests adding distribution provider.
- Need to be clear on the reason for adding distribution provider.
- How much heartburn from industry did we get on adding distribution provider? No much attention paid to it.

Bright lines for load shedding.

- Should we be drawing a bright line for the amount of load to be shed? (HG – yes) but make sure the number is clear, that it is the right number and the steps involved
- This only applies to the portion of assets under NERC scope and nothing else. There are other standards that address load shed
- Are we beginning to address issue not addressed before – should be a primary cranking path
- There is not one and is not in the scope of this group
- "initial cranking path" may be the key term – NERC functional model should determine this.

- An example of physical security as an alternative method of protection – here we were trying to address cabling between separate entities – the Progress Energy RFI was addressing a cable that ran outside the physical security but connected the same location
- Involved six wall perimeters –this is an example of a general protection with added layers of security as required
- This could take the scale of assets to be protected from hundreds to thousands
- If only addressing CIP 002-4 here then do not add

Applicability 4.3 exemption from 002-4 and Facilities

- Eliminate exemption statement of 4.3.1?
- Facilities can mean many different things.
- Does the need for exemption goes away under 4.2.1?
- Systems of facilities within?
- "facilities" refers to those with terminals – careful how we use "facilities" – the capitalized glossary term does not mean just a building.
- For example, nuclear considers everything inside the outer fence as part of the facility – this allows them to include those as "facilities."
- Does this clarify what is in NERC's jurisdiction? Does not seem to add anything. Jurisdiction is determined outside the standard.

Straw Poll

In favor removing 4.2?

15 members favor removal of 4.2, 3 opposed. Passes 83%

- Is FERC okay with that? A: not sure what you are doing with 4.3.1
- That stays out as an exception

2. Requirements section

R1

- Creating a new attachment 1? (Yes)
- There is a request for interpretation on this language already *(participant)* – cable between units in the same perimeter?
- Have separate ESP's
- If one ESP then you have to have physical six wall protection? A: yes

R2

- Should examples be in the requirement? John Lim proposes taking them out
- Support taking examples out and place in guidelines
- Agree to remove, as they do not add to the requirement
- Reviewed the alternative – takes current list of functions and include as attachment #2.
- Breaks R2 down into three parts - each piece is different set of assets to be identified
- Are we re-introducing function based assessment? Given short time frame for posting, not sure we can fully develop this.
- "situation awareness" was a big concern in the industry comments – we need to be able to clearly define it.
- We should include and be able to define – "situational awareness" as a component of every outage
- Trying to get industry to think more about computer connected systems – the industry rejected the Maureen edit of "functions", not what we originally wrote – network computing is what this is all about.
- Concerned about the time this will take in completing our task on CIP 002-4
- Don't add attachment #2 to CIP 002-4 – there is not enough time to develop both attachments and address the push back on both.

- We don't define situational awareness from whose point of view –
- Cyber assets with dial up? We may need to clarify intent and modernize if necessary to include any remote access.
- Without examples of functions, I question the effectiveness of R2

Straw Poll

- How many favor Rich's alternative to includes list of functions as attachment – 5 in favor
- How many favor the original R2 with examples? 6 in favor.
- How many favor the original R2 without examples? 12 in Favor.

- How is entity and auditors going to determine what is essential without examples or an attachment?
- That is what they do today
- R1 is the reason we are doing it
- Keep wording like it is today but in the new world for 010 and 011 we need examples
- May need guidance with examples or attachment 2
- Are we giving the industry an opportunity to shoot itself again – leave in a loop hole here then have an empty critical cyber asset list
- Need to make clear the essential cyber system functions, and we need a bright line
- Agree for more clarity on what CCA's are supposed to be but there is a risk that introducing it here is too big an initial step. We are dealing now with 002, then go back to 003-009 – trying to get industry acceptance.
- Ff it is not routable it is not in scope
- We have been asked to do a minimal scope then return to what we were doing with 010 and 011
- R1 is an eighteen page guideline from a different standards process –
- If a guideline exists, then we should use it
- Even if it is just guidance and auditors can not use it or enforce it
- **Motion (Lim/Brenton) to remove examples and keep remaining language R2 in first paragraph – 14 in favor, 4 opposed. Passes (78%)**

- Separate discussion of 2.1, 2.2 ad 2.3:

- R2.2 –need to expand
- That is a good idea but not for this round as it brings in a whole new set of assets.
- FERC had indicated that the SDT will need to justify why you are removing requirements.
- Without this change we will not head off the politics surrounding us
- It is the right thing to do, it is an update.
- It amounts to replacing all three with "if connected by routable protocols" – may turn into critical assets without any outside connectivity
- Industry may have to unplug assets
- Better than letting outside threats bang on it
- The industry needs to be defending at the host level and on interior systems too
- This is the problem with the 002-4 process – we are balancing what can get past industry and what Congress will accept.
- We still have not determined what we can afford to protect or we will have scope creep
- If advanced persistent threat is what we are after and we remove ability to communicate outside, then why cover routable within the same cabinet?
- Miss list of those authorized to access, also miss out on recovery plans, testing, etc. too – those are the things we need to determine the full threat – all these devices need to be included in a minimum protection scheme.
- Dave's proposal goes in the wrong discussion. Doing something fast is important now – we were on the right path and were told to stop and do something quick, then go back to the right path – cannot deviate and make everything right at this point – true we could make it better but have to get this job done first.
- Need a better update on risk assessment – need a clear cut set of risks to address
- Jim (phone) – agree we need to be more encompassing – note many sticks used to attack routable protocols through introducing viruses without being connected.
- Support moving forward quickly in order to get back to the right path
- For each requirement we need to ask what is the right thing to do, not just expand critical assets by the end of the year.
- We should always ask if this is the last time we get to discuss, what should we do because it may get yanked out of our hands – need to educate industry

- Important to do the right thing and need to secure the system – the next version will be more tailored to the equipment we are using – we need this now to allow industry to regulate itself
- If we use what the threats really are, would require massive education of congress, auditors, industry and others – now we are checking boxes for compliance.
- We can get something acceptable to industry short term in order to get time to do the right thing for the industry
- Cannot be yanked away from us without Standards Committee based on motion of author – the SDT should focus on solving the problem and less on Congress
- Need to play game and find medium to get us there – suggest addressing the dial-up language too.
- This will pass industry – EEI CEO's are whipped up and concerned they will lose authority to regulate themselves – this will not be rejected by industry
- If we put in those changes and it will be rejected
- If we make further tweaks here then need to make tweaks in 003-009 – cannot support change here.
- Would it be suicidal for the industry to ask you to stop and change direction then vote it down?
- The fundamental difference here is we are not just addressing critical assets but trying to improve standards as we go. We will continue to butt into this difference in approach
- Limited scope to change – now changing more – where is the line? Need to work on the bright lines.
- We all want a material impact on identifying critical assets – we need real security, not just paper security.
- Already made changes to R2 which is part of 010 – trying to make it better but not addressing everything you already changed.
- We never reached consensus on what our objective was. We did not change R1 but did start to change R2?
- Way too far to go to change everything and file by December – but changes here go to informing people where you are headed – need to include a list of cyber assets that need protection.
- Changes in R2 to remove functionality impacts in the definition of CCA's – may have removed some and weakened it.
- The issue of list not having enough on it – started with Mike Assante's letter – if we do not fix the CCA list then still have empty list?

- Note that "cyber" does not even appear in survey – it only asks about CAs
- Midwest organization ran the survey and had fewer CAs on the list
- Motion to focus discussion – suggest #2 on the purpose statement list captures what we need to do
- Scott Rosenberger's motion (John Lim second):

The SDT objective for CIP 002-4 is to leverage the work already completed by the SDT for CIP 010 in developing a revised CIP 002-4 version that is narrowly scoped to identify the Critical Assets in the Bulk Electric System through the use of bright line criteria as currently under development in CIP 010 ~~in place of the risk based methodology in CIP 002-3~~

Discussion of the Motion

- Clarifying question? Earlier changes discussed would be negated? Yes
- This represents a principle to help us move through and get CIP 002-4 done
- Friendly amendment to shorten and remove reference to CIP 010? No leave as is.
- The less we say the better – say what needs to be said and no more
- This acknowledges leveraging work done to date
- Should we make entities use bright line within their current process? There should be no need to replace current risk based assessment if we provide bright line
- This motion is trying to make sure we fix CA discussion. We can then consider a separate proposal to refine direction
- Suggest adding CCA? No.
- In Dallas one company said approach then cut their legs out from under them
- Scott is comfortable putting in period after CIP 010 and drop last clause:
- Need to make clear they are inclusive, not options
- Need to replace risk based with bright line?
- SR – that is not covered here – did not want to leave in risk based to keep assets from falling of the list.
- Does this rescind earlier discussion on R2, including deleting the examples?
- Does this include "engineering studies"? (No)
- Very concerned that some at entities who tried to do the right thing will now lose their jobs

- CIP 010 and 011 will bring those back in scope when we get done

Motion above: 15 in favor; 3 opposed. Passes (83%)

- R1, R2 and R3 will remain the same

3. Attachment #1

Below is an overview of the straw polls taken on various provisions of the draft Attachment #1 for CIP 002-4. Following are discussions points on the sections.

The SDT reviewed and discussed and polled the proposed revisions to Attachment #1.
The following are the Straw Poll results:

- Support for dropping 1.1: 15 in favor; 3 opposed. (83%)
- Support for Revised 1.2 language (a-d). Support for – Support 0 Oppose 19
- Support proposed changes to 1.3 - 13 oppose 0 support ; abstain 7
- Support section 1.4 as changed: 14 support; 5 oppose (74%)
- Support 1.5 as revised – 18 in favor 0 opposed, 1 abstain (100%)
- Support 1.6 as revised – 19 in favor 0 opposed (100%)
- Support including 1.7: 18 in favor; 0 oppose; 1 abstain. (100%)
- Substitute in 345kV –5 in favor; 14 oppose. (26%)
- Support 1.9 original language with FACTS and IROLs: Support 12; Oppose 0; Abstain 6 (100%)
- Delete the second sentence in 1.9 –14 in favor: 0 oppose: abstain 3 (100%)
- Proposal to use “control center” – Support 17, Oppose 2. (89%)
- Proposed language without limits for 1.14-1.16: 10 in support; Opposed 10 (50%)
- Support for: “Any control center or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions. Support 13; Oppose 1; Abstain 8 (93%)
- Support for: “Any control center or systems and backup control center or systems performing RC functions.” 17 in support; 0 Opposed Abstain: 1 (100%)

- Support for Approach: Appropriate to incorporate bright line criteria from attachment 1 into the risk based methodology. Support 8 Oppose 12 (40%)
- Support for Thresholds on 1.18- 9 in Favor; 8 Oppose ; 1 Abstain (53%)
- Support for Thresholds on 1.19 10 in Favor; 8 Oppose ; 1 Abstain (56%)
- Support for Thresholds on 1.20. -12 in Favor; 6 Oppose; 1 Abstain (67%)
- Support for taking out distribution provider in 1.15: Support 14; Oppose 1; Abstain 1 (93%)
- Support for Wording in 1.14 and 1.15 from 002-3 R1.25 – "System and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more." Support 14; oppose 0 (100%)

"Nuclear generation facilities"

- It should not matter how we boil water – the fuel source has no impact on reliability – addressed that nuclear facilities have to comply by removing them as an exception – should not say all nuclear facilities, regardless of size, are included
- Nuclear units take twenty-four hours to come back on line – no need to call them out just because they are nuclear.
- Some fossil fuel plants can take up to eight hours to come back on – NRC controls safety aspect of nuclear fuel
- Agree with comments – There is no engineering basis to call out nuclear separately as to reliability – Might include them in 1.2 criteria in some manner.
- We should be forward looking to changes in nuclear and new technologies.
- No technical justification for including nuclear separately – it is all electricity regardless of how it is produced – this is politically driven.
- Some agreement with NRC to include nuclear as critical assets – do nuclear facilities already have standards for their facilities?
- Nuclear safety is covered by NRC – more risk to the plant by the system than to the system by nuclear plants.
- Thought we were handling by saying "a generating unit, including a nuclear generation, …" in 1.2
- This is not in to address any agreement with NRC, rather it is in for political optics – even including in 1.2 appears to give an out for including a nuclear plant as not critical
- We did not make any distinction for any other fuels through the whole standard – from reliability stand point it does not matter – putting into 1.2 says we are listening but not actually recognizing any difference in reliability – that is the purpose of the standards

- Agree with comments – does not matter what fuel is used – may explain optics by changes in the applicability section, but if in the attachment, better in 1.2.
- Prefer putting in the applicability section but may not be obvious enough
- Nuclear is beginning to require cyber security measures in their licensing process – they have a defense in depth methodology in place – may miss on the optic side if only four out of over 100 units are identified as CAs
- Lots of talk about optics – NERC communications director can communicate – let industry know the justification – no technical basis, only political optics – NERC needs to do a better job handling the optics
- 1.11 addresses interface with nuclear that is reliability based.
- The threshold of 2000 for high will not capture most nuclear units that operate in pairs to create 1800.
- Consider naming them in 1.1 subject to criteria listed below.
- Agree to remove 1.1? If so, do we need additional criteria for nuclear?
- Motion to drop 1.1, with removal of exception for nuclear
- If the SDT removes 1.1 we will get comments back on the record from NERC to put it back in
- **Support for dropping 1.1: 15 in favor; 3 opposed. (83%)**

1.2

- Confused – "a group of units" relies on common control system – language is confusing, the concept is right
- Is it the lowest of the three or the highest of the three? Should be the lowest
- There is a contingency reserve or a shared contingency reserve – same thing – matter of total reserve.
- If 2000 mw or lowest value – then drop c.
- A and B are the same thing – combine with an "or"
- 1.2 needs to be more succinct and plain language – also is 2000 MW enough?
- Not the most productive to wordsmith as a group – Jason Marshall offered the Chair agreed to let him take a shot at redrafting and bring back tomorrow for review
- Intent is to capture the cyber systems that are part of the aggregate
- Is 2000 mw the right value?
- There is a logic issue between a, b and c.

- Support creating a proposal – do not forget we may need criteria for covering nuclear
- Needs to be based on reliability
- You have to have contingency reserve in nuclear
- Mike – no single units of nuclear exceed 2000 mw – and no mediums identified here
- Still looking at common or aggregating control systems
- Talking about big iron, share concern about 2000mw
- Those units do not share common control systems – might need to discuss aggregate bus as was described
- What are we protecting against – do not care why I lose unit, just about getting the supply back on line
- Generators themselves may not have common control – but other GCS systems may be in common .
- Comment may be covered by 1.17 which addresses generation control, not generator control
- Generation control is not within the generator control room
- We should be careful we invest in the units that we need to.

At the request of the Chair, Jason Marshall brought back some revised 1.2 language for the SDT's consideration which includes four options a-d

1.1. A generating unit, or a group of generating units that share or are reliant (dependent) upon a common cyber asset (e.g., control system) that has/have an aggregate highest rated net Real Power capability exceeding:

a. the Contingency Reserve of the associated Balancing Authority, or
b. the Contingency Reserve for the Reserve Sharing Group,
c. the associated Balancing Authority's obligation or share of the Reserve Sharing Group's Contingency Reserve or
d. 2000 MW.

Member and Participant Comments

- The 12 months was in there to cover seasonal ratings to keep units form going on and off the list.
- Makes sense at first blush but once on the list you will apply cyber security controls.
- It would allow gaming and the 12 months would limit potential gaming
- Can add it back; just trying to make it simpler

- 12 months limits fluctuation of value – need to set a definite value
- If move things in and out may only be in the interpretation phase and never get to implementation
- I think it adds confusion between 12-month sliding period within the three years
- The preceding 12 months sets the time period
- But compliance period is over three years – this is overly complicated, if any time in the three years then it must comply
- Look at R1 and R2 – words say on that day of annual review
- Sets an anchor – propose keeping the 12 month language to anchor the value
- All assets get roped in as critical assets even those not interconnected
- Suggest putting "that would have an impact on the reliable operation of the group o units within 15 minutes"
- How do we audit time compliance? How do we provide evidence to auditor?
- We can take an asset down and document that event
- Cannot provide evidence you can audit to it
- We are both a balancing authority and in a shared group – looking at "b" we could hit that – "c" is a different value for the same entity, how do I pick the appropriate one
- Says "or" – can choose the lower one
- Does that mean everything over my minimum obligation in "c" must be covered as a high?
- If balancing authority loses your share does that put the system in danger?
- I cannot defend that we have to cover everything over our minimum share if we also have the ability to cover the full reserve on our own
- Concerned about the addition of "c". How does c relate to a? Also concerned that our share under c is but a sliver of the pie. Compliance impacts that could come back and bite us
- Instances of "a" few and far between – "b" more likely – "c" may be lower as your portion of the shared group's reserve
- Still concerned about adding "c"
- Also concerned about "c" expanding obligation beyond obligation under "b'
- Concerned this addresses the reliability of individual entities rather than the bulk electric system – disproportion impact on PA's?
- Concerned about the actual grammar used – the "(e.g. control system)", and also the 15 minutes as equal to "real time"

- Jackie Collett noted she was willing to volunteer to rework the language
- This is confusing as to which direction it is going – for our organization it would bring in about 75% or more of our assets
- Propose b and c are exclusive of each other – either use full groups number or your portion – go with either b or c – your share under c is always lower – suggest dropping "c"
- We would have to go to "d" – for us "c" would be arbitrary

Support for including "c" – No Members

No changes to 1.3 and 1.4

1.5

- Added "primary" to 1.5 – though there is no definition for "primary"
- Last call we discussed the term "primary" and suggested using the term "designated" instead – neither word is officially defined – what wording should we use?
- Blackstart is not about reliability but recovery
- Instead of "primary" –since there are different stages of restoration, focus on initial stage of restoration as the critical moment
- Primary and designated are not the same thing
- Need to be sure designation plans are the right source – hundreds of units included in our area to cover multiple contingencies
- R1.3 – coordination between individual transmission operator restoration plans
- But R1.5 has the assets
- We have to be careful to avoid unintended consequences
- Question about contingency requirement and not meet a or b? Ever not meet contingency reserve in a or b and have to fall under d
- Concern about 12 months – consider prior calendar year rather then preceding 12 months? Variability in what this captures by entity – how do we know what it captures; does it capture the appropriate assets? This is too obscure for oversight as an entity by entity threshold.
- There are three or four ways to say the same thing – needs to be one number to meet whether as a single unit or in combination – propose one value for 12 months – conversation should be on the right number, not how you get there.

- Comfortable with removing “b”
- If we remove “b” we need “d”
- Concerned about removing “b” – confusing if we are left only with “a” – who is the associated balancing authority?
- Agree cyber system needs to be protected but do we mean that the small pieces that add up to the whole are each in themselves critical? The generators themselves are not critical.
- Nuclear – it is the control system we are trying to protect.
- May not be the right approach for the generating units.
- Trying not to lose control system by looking at individual units.
- This says the individual units are critical if they aggregate up to a critical level.
- Have to take the units as a group and look at the system critical for running that group – not the individual units.
- Does the wording here say that? May inadvertently be focusing on the individual units rather than the control system of the group.
- Bringing in every system for each unit which may not be critical.
- May need to look back at possible link to R2 as well.
- Remove the part discussing the combination of units, go down to 1.17 and add any system controlling the aggregate of units – possibly added as 1.18?
- This list is trying to identify which generators are critical to maintaining the reliability of the grid –
- Delete “a generating unit for” to be sure not looking at individual units and focusing on group. Also make the subject “common cyber asset” though that may not help with political optics of identifying more assets as critical.
- Phone? – adding language in “a’ drops the threshold to a low number bringing too many units into play?
- Goal is to protect the common asset – strike first sentence up to “upon.”
- Can you have a reserve less than the unit?
- Think about what we want for the outcome – do you want the group rather than individual units – focus needs to be on protecting cyber systems not the generation units.
- Talking about the bulk electric system reliability and the cyber systems that are connected to them.

1.3

Member and Participant Comments

- Why 1,000? What is the rationale?
- Best number we could agree on using our professional experience, expertise and judgment.
- 1,000 seems arbitrary – need to reword to tie to RC and not tie to a number – add "any reactive resource listed with in a mitigation plan approved by the reliability coordinator."
- The RC does not decide what equipment should be installed – also need to substitute NERC glossary term for the mitigation plan – need to be an operating procedure and process rather than mitigation plan.
- How hard or would it be possible to write up the reasoning behind the number? Bright lines are arbitrary with some rationale behind them – is this a work product for later?
- Documenting the rationale helps flesh out the petition to oversight authority.
- Trying to understand the impact of the proposed language – how much stuff would be coming in?
- Will it be clear which operating procedures will apply? Which ones belong to the RC's? Test new 1.3 language?
- Provides more of a rationale than the arbitrary number.
- Like to add "required" operating procedures.
- Are plans "approved" by the RC – change "approved" to "required."
- How does the owner find out what is in the RC operating procedure?
- RC has to communicate those procedures.
- Concerned about how logistics would work – bright line was easier to determine what this applies to.
- Add "Operating Procedure, Operating Plan and Operating Process"
- Will have many requesting plans that may not be related to this issue.

Straw Poll

- **Favor changes to 1.3 - 13 oppose 0 support ; abstain 7**

1.4

Member and Participant Comments

- Concerned about impact – not understanding or it is not worded correctly – looks like everything would be medium – also "Wide Area"
- "Must run" is a market concept and should be deleted
- As used here reliability is not a glossary term – reliability "must run" is distinguished from market concept – put back in in response to comments, need to clarify it is there for reliability purposes – need to keep track of the rationale
- Will Maureen let us get away with the quotes?
- Longer than the implementation schedule?
- May be there until a transmission or generation unit can be built
- Appropriate to say "pre-designated by the reliability coordinator as …"
- Still concerned about using "Wide Area"
- It is not always the planning coordinator – pre-designated covers both if not as clear as adding reliability coordinator
- Planning coordinator is responsible for coordinating with the asset manager – replace reliability coordinator with the planning coordinator
- What does pre-designate mean? Strike in favor of "identified by the Planning Coordinator."
- Can we eliminate "Wide Area reliability impacts"?
- Keep developing in passive voice – planning coordinator identifies as…

Straw Poll

- **In favor of section as changed: 14 support; 5 oppose (74% Passes)**

1.5

Member and Participant Comments

- Delete "primary"
- Could be unintended consequence of reducing the blackstart units covered
- Agree – another suggestion – no basis for primary, and language is redundant –
- Alternative – Blackstart Resource and the Facilities comprising Cranking Paths contained in the transmission Operator's restoration plan
- Can also use tie line to restore – not covered here
- Cranking paths include tie lines?
- Facilities as capitalized is defined – do we need a more specific level?

- The language here covers each of the issues discussed
- I read it differently because of the "and" means 1.5 does not apply at all – suggest two items
- Blackstart resources is well defined – let stand alone
- Any Blackstart Resources contained in the Transmission Operator's restoration plan.
- The Facilities comprising Cranking Paths contained in the Transmission Operator's restoration plan

Straw Poll

- **Support 1.5 as revised – 18 in favor 0 opposed, 1 abstain**
- **Support 1.6 as revised – 19 in favor 0 opposed**

1.7 – New

Member and Participant Comments

- Optics type criteria added
- No problem with the requirement but question the optics –
- Regional issue to define
- How do we handle the fact that NYC is not covered – bad optics
- Need to have a technical reason – if just adding for optics, we will get called on it
- Not every criteria has a technical reason or justification
- Many industry comments asked for technical reliability based reason for various criteria – need to be able to say why this was put here beyond perception
- Rationale: to protect the back bone of the system
- Do we have anything in writing to put this in here? If we pull it out, will we get a response or directive to put it in with a rationale?
- In CIP 010 we said had to have "four lines" – how do we do that later with 010 if we put this in here?
- With some research could create some rationale – critical to us in Florida – need something to support putting it in
- Team did not include this, but NERC staff did in response to informal directive – I do not have an issue with including it – clearly critical at this level
- This may be arbitrary but it does not hurt us and should be included, just with some justification beyond political optics

- Support including, goes with 1.8 – if you take 1.7 out then would need major rewrite of 1.8
- Including is a good idea – engineering analysis may not justify but collective experience of this group does
- No problem with 500kV, but need more than political optics to hang our hat on

Straw Poll

- **Support including 1.7: 18 in favor; 0 oppose; 1 abstain.**
- **Substitute in 345kV –5 in favor; 14 oppose.**

1.3 and 1.4

- 1.3 – "reliability coordinator" – RC does not require anything, not part of his job, just enacts guidelines passed to him – and, "mitigation plan" is a compliance term
- We know how to operate the system but may not have the language to properly explain it – "require" may not be the right word
- Majority of plans are for coordination – if trying to identify assets, then need to look at other documents, not to the RC
- Look to responsible entity's
- Look to the definition of "operating procedure"
- Put in "owned by a registered entity" and "submitted to a reliability coordinator"
- Doesn't add anything
- Some RC have copies just in case not because it is critical – "invoked by the RC"?
- Way it reads now it includes any reactive resource
- Only those submitted to RC to address and issue
- Will take back to his RC

1.8

Member and Participant Comments

- Syncer phaser requirement?
- Many – nothing to do with it
- Texas interconnection but run by ERCOT
- Needs to say "Texas Inter-connection"
- Same for Eastern Interconnection and Western Interconnection

1.9

Member and Participant Comments

- Strike FACTS
- But that is how you define an acronym in a document by spelling it out followed by parenthetical
- FACTS is well defined – question removing it – serve a real purpose where they are located
- Make it a line item for just FACTS
- Used to have a separate item for FACTS and IROLS
- Do we need to delineate into separate items
- Not sure if we need to delineate, but recognize to avoid unnecessary comments
- Reason for choosing IROLs instead of SOLs
- Is there a critical link between FACTS and IROLs? If not, then separate

1.9 original language with FACTS and IROLs: Support 12; Oppose 0; Abstain 6

Member and Participant Comments

- Why include Cascading – seems like the line is not bright here
- Because of the definition and inclusion of IROLs here
- Define FACTS
- We define only if it is different from commonly accepted definition or need for clarification in the industry
- Do not capitalize items unless they are part of the glossary
- Agree this looks sort of like a study – not many studies look at misuse of devices – support including FACTS devices but consider as a separate item
- By tying to IROLs it raise key devices without putting in more than needed if FACTS devices are separate out as a stand alone item
- We can simplify this and clarify coverage
- We could drop the whole second half of the sentence
- Need some delineation because not all of the FACTs devices are critical – they are local area things, not critical to BES reliability
- Add “outages” after Cascading
- Not needed

- Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that , if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating limits (IROLs) – simply drops the second sentence
- But some areas do not have IROLs
- Recommend keeping the second sentence in
- Same concern – keep it in
- Need to change the second sentence if it remains
- Not available or not identified?
- Do both sentences say the same thing – does anything fall out if we drop the second sentence?

Straw Poll

Delete the second sentence –14 in favor: 0 oppose: abstain 3

- May be a compliance issue in areas without IROLs.
- Have to have studies to show they do not have cascading problem.
- For compliance, you need the second sentence.
- End of first sentence add comma and "would result in instability, uncontrolled separation or Cascading."
- Looking at different definitions and comparing the language.

1.10

- This is similar to 1.2 which we changed and are still revising
- Do we need to wait and see what we get there?
- Jackie Collett will edit 1.10 to include or conform to changes in 1.2
- Bus tie breaker? Do we need to include the breakers?
- But it is the transmission facility
- If interconnection occurs at the breakers, then include – it is for the utility to decide where the connection is.
- Suggest we capitalize Facilities and add "and Elements" which by definition includes breakers
- Do we need to add "Elements" to other areas we have "Facilities"?
- Facilities is a collection of Elements – add here but not above in 1.2
- Do we need "Transmission" at the start of the sentence

- Looking at transmission substations – just say “Facilities”
- A collector bus is a “Facility”
- Call out generation too – begin sentence with “Transmission Facilities and generation Facilities”
- Identified in the generation interconnection agreement

1.11

Member and Participant Comments

- Does it need to be called out? Can we reference another standard in the standard?
- Best not to reference another standard, put period after “Requirements” since NPIR is a defined term.
- Consider moving this up to the other nuclear item
- The other item was deleted and also we were trying to keep generation items together.

1.12

Member and Participant Comments

- Does local area create problems?
- Put language in due to the lack of a clear definition
- But what does it mean?
- Don’t think NERC definition will help
- We had a great deal of discussion before landing on the existing language as a compromise
- What about using RROs?
- Not everyone has an RRO
- Concept of local area is important to capture

1.13

Member and Participant Comments

- Does this change the meaning under CIP 2-3? Does it bring in the smart grid? What is the source of the 300 MW bright line?
- Bright line written for 010 – may need to rewrite here – as for smart grid, intent was to capture it going forward as it involves dropping a block of load to protect the reliability of the BES – we say automatic aggregate load shedding but not how or why

- 300 MW came from DOE 417 – also, what ever system can initiate the dump is critical, not the individual units that shed the load (unless it can unload 300 MW by itself)
- Grammatically say automatic load shedding in the aggregate?
- Will review language
- Would collection of small loads constitute high impact?
- Need to determine if system controls 300 MW
- Do we need to also cover a BES element that could draw 300 MW?
- Any BES element that can result in over 300 MW loss is covered
- Any control center that is capable of controlling more than 300 MW of load?
- Control system, yes – not just control center which also would be covered
- Operator versus automatic – the former is not covered, only the latter

1.14-1.17 were combined and have now been separated out

Member and Participant Comments

- The way this reads and auditor could read everything inside your fence is critical asset
- Need to change the word center to system
- For RC need to say situational awareness
- We have not adequately defined situational awareness
- As it stands you will greatly increase the devices covered –
- Term control center is vague – guidelines help but are not applicable here
- Primary system or backup system
- We are still in the old original paradigm – we are protecting the cyber asset – what is essential to the control center to ensure reliability of the BES? It is the control system – the issue is resolved in the next version of 011
- Have to include 1.14-1.17 to be sure central control centers are included
- Concerned we have added many assets we do not need to
- Leave as is, most will understand what is included in the control center
- Backup center in large building but sequestered – this is not a problem
- Assuming the next set, 010 and 011, will follow soon after this version but understand this version may be in place for awhile

- We are describing things by physicality rather than function here
- FERC needs to understand entities expense in time and resources to meet current standards, this new interim one and then subsequent 010 and 011
- Where does the control center begin? It is not the building or outer fence – need to identify where the BES assets that control the system are located
- Control center is a different issue for critical asset while control system is critical cyber system – each entity must determine where the control center is
- If you can define your control center – we had to use systems to define criticality because we could not define by physicality – not acceptable to determine how we have to define our control center
- The building is not the critical asset
- For CCA's in subcabinets – how controlling the cabinets
- Have a physical perimeter around cabinets
- Proposal to change center to system? I have not heard any concerns
- Many expressed concerns about changing
- We have many control systems – they do not perform the function of the control center – control systems do not capture the intent of this section
- Identifying critical assets not critical cyber assets
- Proposal to change from one undefined term to another undefined term
- Critical assets is a defined term – includes systems

Proposal to use "control center" – Support 17, Oppose 2. (89%)

Comments after Straw Poll

- Concerned about stripping out base for control centers – if remove BAs then no impact
- But need to account for misuse, malicious or not
- We need a bar, a bright line
- We stripped out those limits, bars, etc. – need some limit on identifying "critical"
- "Performing"? Are they registered? Or responsible entity?
- The language here brings in too many small entities and may exclude large entities controlling several small
- If you want a bar, you need to state what that bar should be
- Go back to high language we had before

- Remember 911 attack came through Bal Harbor to get to Boston
- If we keep this language then we keep in medium when we move back to 010.
- The control system is the key asset we are protecting – sophisticated level of attacks means we need to do more and have more robust protection even at small or remote sites – need to add "registered" in front of each entity identified in each of these – need to be sure people performing the high risk functions are asked to do more
- Jay – recognize were we are in the time line – we have to do a little optical maintenance at this stage
- In 011 we should force protection for all iccp's across the board
- Now telling those who used systems go back to big iron approach only to be told to go back to systems approach with 011
- Suggest striking 15-17 here and address using systems in 011
- Need to accelerate protections while meeting political expedience – get people moving in the right direction with the first step
- Control centers are covered in 1.2.1 – cannot take it out at this point
- FERC position – if new version removes requirements then it needs strong justification
- Current 010 identified high, medium – if make everything high, then cannot go back
- Size with control systems does not matter – only matters for big iron
- Propose adding back in language for 1.15 and 1.16 – to preserve option for high and medium in the next phase developing 010 and 011
- Not okay to use system to scope down but can for size of asset?
- If include language used in Dallas workshop, we need to include justification for the commission
- Talking about critical infrastructure – this is not a new thing
- Is there any tweaks from the workshop or comments we need for preserving the high and medium as we move to 010
- Still need to document justification
- When we did 010 we separated high and medium, in 011 we moved much of medium up to high
- When we get to 011 we will add more to high than are currently in 003-009
- Should we have a level? If so, maybe we need to determine the bar or line for each level

- What would we not do for medium level control center that we do not already do for a high control center
- FERC has said cost is not a justification for not doing it – propose we test language as offered here without going back to previous language

Straw Poll- Language as offered without limits for 1.14-1.16: 10 in support; Opposed 10

- Proposal to start fresh tomorrow?
- Concerned about having to cover as critical units that are not connected to outside units that collectively have less than 200 mw impact should be classified as critical and require high levels of protection
- Small cities with limited connection do not have a high impact on the BES
- Are they a BA or a generation control center?
- Can we ask John Lim if there were any additional edits to incorporate to limits from comments at the workshop or responses to industry comments
- Legal also concerned about the language in the survey – agree with the changes proposed by the team but make the change for the posting of the survey and the cover letter
- Does the team have to make a formal comment to make the changes happen
- Comment on the survey is open but not the data collection – board will approve the survey and will have the final version of 002-4 to base the survey language on – better to let staff make changes to survey language without the formal comment

Control Centers

- Should we look at Jackie's updates first
- Joe has the changes to present
- This is a criteria for figuring out what is needed for reliability of the BES not cyber security – then figure out what cyber security system is attached
- Then we should change the title to "Big Iron with computers attached to it"
- Reviewed suggested revisions – also change cyber system to critical asset – highlighted changes with blue – Word changed the numbers.
- Last time we posted it had the clarifiers on the thresholds, what comments did we get back?

- In 1.18 at the end is an “and” that needs to be an “or”

New 1.17

Member and Participant Comments

- What are we trying to solve, what does this do for us – we would fall out as a balancing authority – this would drop us out for a short time until we revise 011 – may not be as a big a deal not to have the qualifying criteria as we discussed yesterday.
- We have small systems that does not impact anything – not all control centers are the same – this becomes the high going forward and will remain so in the next version – many other small entities will have the same problem.
- Stay focused on what we are doing in 002-4 – not necessarily the case we will be stuck with the change – we may need to scope the controls at the component level instead – focus on this for now and not try to predict the future by looking into the crystal ball
- Are we implying there are other control centers not included? Even if a control center currently is or could be used to control the system it should be covered.
- Agree with RC – not putting any limits in 1.17.
- Current language in 003 causes problems – title of this is critical cyber assets – it is not about control centers.
- Backup control centers are not captured here.
- What about backup control centers – backup has baggage to it.
- Change to any control center that is or could perform RC functions – capability to perform.
- How big an issue is it for entities to identify primary and backup control centers
- Backup center is passive, it does not control anything, but watches – we declared control systems as critical assets used to run the iron.
- Multitude of control centers that do not run reliability of the system
- But should be if it performs any reliability coordinator function
- What does RC actually do – only 17 in the country – seems obvious that what they do is essential.
- We have no skin in the RC game – makes sense if registered as a RC or through delegation – Entergy used to be an RC but not now. Should they be covered?
- Any of the members could be an RC – should remove ‘with capability’ and change to ‘which.’

- Capability could be an avenue to attack whether you are actively using the capability currently or not.
- Concerned that we do need "capability" – narrow down from capability but need more than just active current ability.
- Most RC's have smaller staffs.
- But RCs are powerful in that they give directives to others – consider "host RC. functions" – trying to get at those who can give directives – or "designated" – also, can we get away from concept of it being a place or room by saying "equipment"?
- Concerned about removing "centers" – may be able to add "systems" but cannot remove "centers"
- What about systems that support the control centers such as fire suppression systems – are we trying to include them.
- "Any control center and its systems that are designated to perform the RC functions"
- Many have capability – trying to capture those who are doing it or have backup to do it – designated covers that with too broad "capability"
- "Designated" better but still not sure right word – not sure we "designate" a system, but do use them for that function
- Who and how RC functions are done varies between regions – designated may be vague in our area – prefer "capability" as capturing the essential functions.
- Functional model is not clear in the overlay of the system – say the "computers used"
- "That are used by a registered RC or its delegate to perform Reliability Coordinator functions.
- Control center or its system – you get the choice to choose which one, not required to do both
- "Or"? Systems needed to perform RC functions include the air conditioning system?
- Not a reliability function.
- Scoped out when looking at critical cyber assets.
- "used by…" is inclusive but could be simplified to say "used to perform."
- SM – need the additional language to capture everyone
- JM – instead of registered should it say NERC registered – who registers RCs? Say a "NERC registered entity"
- Suggest we use "used to perform"

Poll language: Any control center or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions

Straw Poll

Support 13; Oppose 1; Abstain 8

Comments on the Poll

- Concerned about "could be used" – sounds too vague
- reliability coordination is not a glossary term, change to Reliability Coordinator functions
- "or could be used" is not needed.
- Every entity needs a plan.
- Do we need to add RC emergency plan.
- "Could be used" opens it up too much
- How about adding "including backup control…"
- Raises concerns
- Include "emergency plan" instead of "could be used"
- "identified in the emergency plan"
- "reliability coordinator plan"
- That is a different plan
- "that are identified in an emergency plan"
- Need to simplify to used by
- Need to captured what they plan to use – protect the stuff they need to use in an emergency
- "Or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions, as identified in their operational or emergency plan"
- Why include "or could be used."
- Not required otherwise to include them.
- This is still about RC functions – drop the "operational or emergency plans" – adding words that will confuse
- Agree may limit confusion
- Test again without last phrase: or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions?
- We figured out that once system comes on it must be compliant

- Requirement for RC to have emergency or backup is already covered elsewhere – "that are used by."
- Any control center or backup control center that performs a RC function – that is simpler and clearer.
- Have to add "or control systems"
- Control systems do not perform functions

Any control center or systems and backup control center or systems performing RC functions

17 in support 0 Opposed Abstain: 1

1.18 as rewritten with the language above

- If we use this criteria we are dropping out up to 25% of critical assets related to BAs and that makes for bad optics – many munis who are doing the right thing would not be covered
- NERC registry has 139 BAs including Homestead, New Smyrna Beach, Reedy Creek and several other little cities around the country – do we intend to include them as critical – supports having criteria, but are these the right ones
- Thresholds are okay, but we need to discuss the thresholds and not just the words that go in here
- Some drop off, but are some others added in? This keeps anyone form simply saying they are too small and do not need to respond
- Existing standards allow someone to put more on that they think is important than is required
- No one would do that – they would not accept the risk – also related to the BA function, think we should not have any qualifications
- This is why in the original effort we allowed to identify as important but at a lower level – should we have limiting factors, if so, then decide where the bar should be
- Whatever limits you set needs support of justification.
- Put in bright lines and we may take many out – we should wait and put bright lines in the next version
- Current system lists a lot more entities than BA, RC, and TO
- We are changing from a risk based system to setting bright lines
- But many more entities currently have to determine whether they are in – IA, Transmission Providers, others, fall off the list – need some justification for the change

- Difference here we are talking about functions not entities
- With limited scope we are trying to set maybe the bright line is not the way to go
- Justification is short hand for explaining why this is better, especially if the appearance is to drop assets off – simply a rational for the change
- Drop all of these and simply say any control center or backup or systems used to perform reliability functions
- We have never done a sufficiency analysis on any of these items – protecting bulk power rather than protecting the grid – need sufficiency analysis on any bright lines
- I would vote against the limiters in the proposed language – not in favor of removing mandatory control only because entity is small –
- FERC is looking to industry expertise to set rational levels and the reason for them
- Working under order to have more CCAs and CAs – wait for 010 and 011 to help reset levels
- Goals to have more CAs, though more CCAs may have been implied – need to see survey results to know if 002-4 gets there
- Who has cyber asset that if compromised would have the highest impact on the reliability of the BES – those are who we need to target and set criteria to include
- With limits we were trying to match the bright lines set above to identify CA – control two or more of the critical assets identified above
- This is not about size but attack vectors – doesn't matter how big they are
- CIP has always been backwards – working from figuring out what is in or out then setting criteria – here we are trying to work backward from 010 and 011 – need to determine the risk first
- Would it be possible to still include risk based and add bright lines to augment the list of those already covered under risk based
- This is set up as CA but trying to get to critical cyber assets – small control center that is not connected, then out, but if interconnected then does not matter how big you are – may want to put in additional language to cover
- Test simple concept: check on whether limitations should be included, if so, then discuss what the limitations should be
- Are we going to look at telling entities they conduct risk based assessment with the limitations as a minimum
- Modifying the current risk based assessment with these minimums – have to include these at a minimum

- The charge was to replace the risk based criteria with bright line – that is a deviation from the request that would need to be justified – request came from the call with Mosher and Adamsky.
- There is nothing in writing – we are working off the agreement we voted on in the July 2 call
- Perception of NERC executives direction was to replace with bright lines
- Long discussion on these sub requirements – ultimate goal of this group is a standard that adds critical assets to the list, if we don't, it will not be accepted – focus on adding more assets.
- My company was okay with keeping risk based and adding bright lines
- Given direction but were not told alternatives for achieving the outcome should not be considered – this meets the same goal in a way acceptable to the industry
- This method would increase the number of assets which is the goal.
- The associations asked for bright line criteria – we have brighter but still fuzzy lines – careful we do not end up decreasing the number of critical assets – our job is to accomplish the intent to increase the number
- The request may not have considered that some might use the new criteria to reduce the number of critical assets identified – the option here is a good compromise to accomplish the intent of the request
- Using bright line does not make sense – either have to use a methodology or a set of bright line criteria – one or the other, not both
- Data survey request structured to help us make this decision later – it will give us the data to determine which method ends up with which assets
- We were asked to create bright lines, let's finish it – the methodology will require months to prepare
- Not sure survey will clearly establish which assets are identified by bright line versus the methodology
- We can take a high cut at it, without identifying individual entities, by looking at the gross numbers
- Suggest taking R1 from 002-3 and adding "and at a minimum contains the bright line criteria contained in Attachment 1."
- Considers and includes other things – "and as a minimum…."
- Concerned about how this is applied in the real world
- The "bright line" is just additional criteria for you to apply in addition to their existing evaluation methodology – a methodology + process

- Most entities may rewrite their methodology to include the bright lines –
- The difference is that it gets additional message that criteria they were using in the methodology was not tight enough
- Concerned about mixing methods – telling them this is the answer we want you to get whatever methodology is that you use – you may go down if the bright line is in the wrong place – will we get enough granular data to know if number is going down
- "and as a minimum applies (or satisfies) the criteria."
- This does not work for me.
- You have criteria as minimum to include in risk based methodology.
- Keep R1 the same and add bright line augmentation in R2.
- Concerned we will confuse entities – asking them the keep existing methodology and add minimum criteria – if asking them to keep what they have then ask them to use the same criteria without adjusting the methodology
- In NIST had language to use risk based criteria and basic criteria – treat the latter as the only thing they can concretely identify
- We are working on 002-4 because the risk based methodology is not handle properly or has been insufficient at identifying critical assets – we are not fixing the problem but only putting on a patch
- Auditors only identify you have a methodology not its sufficiency – this would allow them to do so
- List bright line criteria in R2 and put the proposed language in as R3
- Presumption that methodology doesn't change from year to year – add "any previously identified assets" to keep entities from changing their methodology
- This is important tool but don't even know if we need to do this until we get the data – focus on getting the right data first
- Risk based methodology is not frozen as risk shifts.
- R1 stays the same
- R1.1 stays the same
- R1.2 Or, create a new sub-requirement in parallel here to speak to attachment as minimum that must be captured by entities risk based system.
- R1.3 The risk based assessment shall consider the following assets: (with list)

Approach statement – appropriate to incorporate bright line criteria from attachment 1 into the risk based methodology

- **Support 8 Oppose 12**

- Important to understand why people opposed
- Need to spend time more constructively
- We either have limitation language or not for all of them
- But we have not even looked at 1.20 yet
- Take them one at a time
- Check on whether limitations language should be included (if so, then discuss what the limitations should be)
- **On 1.18- Support 9; Oppose 8; Abstain 1**
- **On 1.19- Support 10; Oppose 8; Abstain 1**
- Willing to accept limitations if entities could continue to use risk based methodology
- Instead of methodology – another line item saying "any other assets essential to reliability…"
- We want a process that includes CA identified today, anything else you want to add and the minimums of the bright lines – we need ideas to accomplish the goal
- Request poll on twenty (1.20) too?
- Abstained – recognize need levels in identifying CA – trying to narrowly scope and fix in the next version – can we come up with good thresholds at this point in time – reluctantly willing to stick closer to what is in the existing standard
- That may be where we end up but need limits in the survey to give us information what falls above or below
- Political optics of rising and falling numbers
- The Vice-Chair proposed a team of John Van Boxtel, Doug Johnson, Scott Rosenberger, Jim Brenton and Jackie Collett to review and prepare an alternative proposal.

1.20

Member and Participant Comments

- Suggest changing language – Automatic Generation Control is a glossary term
- Changing that term in another committee
- AGC also include operator doing generation control?
- No, definition says equipment

- It is the system that is controlling from a distance
- AGC is becoming cloudy as entities shift how the handle this – some may control in their control room
- Everything else in this area is a functional model – "used to perform the Generator Operator function" to make consisted with the others
- Where does ACE control fall in this –
- It is covered under Balancing Authority in earlier section
- Threshold as written is very low

Straw Polls

Thresholds on 1.18- 9 in Favor; 8 Oppose ; 1 Abstain

Thresholds on 1.19 10 in Favor; 8 Oppose ; 1 Abstain

Thresholds on 1.20. -12 in Favor; 6 Oppose 6; 1 Abstain

Jackie Collett brought back some revisions for the SDT's consideration on Thursday afternoon.

Revision to 1.2

Member and Participant Comments

- 1.2a and b?
- talking about two different time periods
- Contingency reserve different? Should both be Balancing Authority?
- That's where we ended yesterday
- Difference between what it is rated to do and what we actually do – never try to get to capability level
- Think they are talking about net dependable capability – gross minus axillaries
- Make as a recommendation without input or explanation from John Lim who is not here
- It is net Real Power capability – addressed in MOD 24
- Is this the time to discuss 1.2a? Brings threshold down to units over 200 MW – individually a very small amount,
- Should say a reserve sharing group – at least an "and/or"
- Three levels to ensure capture key assets
- Still calculating your contingency reserve as a BA, then figuring out shares
- Requirement as a BA may be lower than the total of a shared group

- Is premise for a shared group valid in cyber system attack
- Contingency reserve for BA bigger than the total for the shared group? The opposite
- Say which ever is the larger of the two.
- If go to the largest, then the 2,000 number becomes the criteria.
- SR – but only if you don't have either the BA or shared contingency categories – instead of the "lowest" use the "larger" of the two or the 2,000 with "total" in front of load share
- Anna – 1.2a should read "the greater value of the Contingency Reserve requirement of the associated Balancing Authority or the Reserve Sharing Group…"
- Have to have one of them
- Went to "lowest" to get the lowest from the previous 12 months
- Can we delete "b" and "c" and just have "a"?
- Like deleting b and c then breaking a up
- We are not saying what the contingency reserve should be but that you can use it
- We are interested in the "high" level – otherwise we get lost in the weeds
- Never have a single unit that exceeds the total
- No single unit is essential to the system
- Offered replacement language for "a" – The CR requirement of the RSG of the BA that is not a member of a Reserve Sharing Group – picking the one number you have rather than the higher of two possible numbers
- Goal is to set a threshold – the threshold we are after is the larger number
- Entities under identifies units because they can move load around without any one unit carrying the load – the size of the unit does not matter
- This is not about how you carry your reserve
- Reality is that type of fuel does not matter and no single unit matters to reserve capacity – the issue of concern here came from separating the two – consider putting back into one
- Lean toward deleting 1.2.a
- Work on 1.3 – if not needed then delete 1.2a
- These were one point before – pull back to just one single number or bright line without need to determine which one you fall into
- Support return to a combined criteria

- Put unit or group of units back together
- What we have said is that no single generator (including nuclear) is considered critical
- No single generator is critical because of the contingency plans
- Point out that under this language no singe or nuclear plants identified as critical assets in the United States – since no nuclear units share control centers – be prepared to state and justify that fact
- No single unit is critical based on size – may be critical for other reasons such as as a black start unit
- Order says n-1 approach will give us nonsensical approach and that saying single units are not noncritical by size – isn't that what I just said
- Need to give NERC or FERC the language they need to explain why a nuclear unit is not "critical"
- That is where we were going with 010 and 011
- Assumption is that 002-4 is not to address the Order – that is the 010-011 effort which will put protection on all units
- The goal to get more big asset generation on the critical asset list? Pick a number to get a correspondingly higher number of units on the list?
- Consider using how much a unit produces over a year

Revisions to 1.9 and 1.10

Member and Participant Comments

- 1.9 – are we trying to say there is an area that does not have IROLs? I don't have them, so then I have to run studies on cascading
- Recall that is a null set that does not require a study
- Okay with taking that out – the whole second sentence in both 1.9 and 1.10
- No objections to the remaining language

1.11 - Same issue we discussed above

1.14 and 1.15 were one item before – split now to BES Elements and aggregate automatic load shedding

Member and Participant Comments:

- Distribution providers in smart grid? Smart meter network would argue not designed to dump load? Should it say "capable of performing" rather than "that perform"?
- May need to lose the word "automatic" – automatic load shed is different from capable of -need to decide to use one or the other, but not both.

- Reluctant to drop the automatic load shedding –
- If we stick with "or" then change common Cyber Asset.
- Tried to capture with common Cyber Assets
- 1.15 is more important
- Support keeping both 1.14 and 1.15 but prefer keeping them simpler – too many words, need straightforward sentence
- Lots of different ways to shed load – the drop due to automatic shedding is what we are getting at here.
- Does the wording in 1.15 automatic include unintended assets?
- Does it include 300 MW of air conditioners when we turn up the thermostat? A: Yes, under the current standard – the concept has not changed
- Distribution providers were not included – only the transmission providers were covered
- If dumping 300 MW – suggestion to remove distribution provider?
- Could you put in an exception in this requirement rather than remove from the whole standard?
- Example of creating interim solution after developing a better process – not fair to say do it this way for now and we will change the rules on you again soon.
- FERC only has authority over bulk power, not distribution.
- Actually for bulk system reliability –
- This is not related to CIP 003 – we need to keep eye on the ball
- We put distribution provider in then out and back again – concern is in the load shed?
- This is new stuff added in to interim step?
- This is a new introduction with big implications

Propose Take out distribution provider? Support 14; Oppose 1; Abstain 1 (93%)

- Much in the news about smart grid and dropping load shed – will be a question we will need to address in the future.
- Wording in 1.15 – propose putting in the wording from 002-3 R1.25 – "System and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more."
- Need to address in 1.14 too
- Could we drop both 1.15 and 1.14 in favor of this language.

Support this change in wording and drop 1.15 and 1.14:

- **Support 14; oppose 0 (in the room)**

Preamble under Critical Asset Criteria

Member and Participant Comments

- I like the additional language upfront but what if facility has no impact?
- Concerned about including invites argument that a particular facility has no impact
- Read current definition of CA – do industry a disservice if we use different wording here
- Take a look again at 1.9 and 1.10 language – left the language in here
- Gives someone capability to declare an asset – they may want to keep it on their list and then drop later with new version
- Goes along with risk based assessment

Jackie Collett brought back a report from the evening session. She noted the purpose was to provide a version of 002-4 to go out with or inform the survey – trying to get information in the survey to help inform the final version of 002-4. How do we preserve critical assets already identified and build on that set? Give entity a chance to identify a list that will stay on for a few years before having to change it again – allow them the option of putting on assets that may not be required as well as require a minimum – keep those on the list from the risk based methodology in addition to a minimum set.

She suggested that the SDT should keep in mind the big cost is getting something into compliance. Once that is done, then it is the cost in maintaining compliance due to compliance exposure. Preserve what is already identified by current risk based. Question for Howard – how much can we change the data request form? May want to add specific questions to help inform team to tweak draft for final version. (Yes, some flexibility to modify data request)

Member and Participant Discussion

- Can we figure out how many assets are added beyond the current base, but not what those assets are – that would go beyond a simple data request.
- Ask for three sets of numbers – number of current assets identified by current risk based methodology, number by category (current CIP 003-009), and estimated total identified using attachment 1 in place of risk based methodology

- This exercise is to deal with perception that not enough assets are identified under the current system – develop a threshold and modify R2 category to identify the common cyber assets for the groups of units rather than individual units – interim phase to move toward 010 – captures more generation assets – question about whether it would apply to transmission, etc.
- Look at current version of 002-4 – how do we capture those concepts?
- Modify and add words from 002-3?
- Any previously identified assets not captured by bright lines need to be sure do not drop off.
- Focus on cyber assets in generation – in transmission?
- Came up with criteria for generation – not sure applies to transmission
- Routable protocol in control center is included – do we need a similar substation or transmission criteria - deleted "in its assessment in 1.19."
- 1.20 Any critical assets that are identified in the last 24 months that are not identified in the bright line criteria – buts a time limit on when I can stop using risk based assessment
- Don't think it is a disaster if those assets fell off the list – will be captured later under medium.
- Take off list, list is too small and list requirement may come back even worse
- What happens if the 010 and 011 are not in place within 24 months?
- Those assets fall off – incentive to complete next version.
- Data request helps determine if we need that item or not.
- FERC put out metrics saying to respond to standards work within 18 months.
- There could be many scenarios in which 10 and 11 are not in place in 24 months, not just FERC approval.
- Wording of 1.20 – have to go back two years to see what was on your list or what is on list now stays on for next 24 months?
- The intent is the latter – do not want to lose ground.
- These words imply the former – need to clarify or modify.
- Add "in a risk-based methodology.
- Don't have to specifically ask what drops out – based on this language are we maintaining risk-based? If not, then say "any CAs identified in CIP 002-3 will remain on the list for the next 24 months…."

- Understand 24 months but puts pressure to ensure next version is in place in time to prevent anything drops off
- Bringing the results back? Rather run the risk based methodology
- Running RBM or anything else you want to add doesn't guarantee anything – if trying to keep CA's on the list, doesn't guarantee it.
- If get to re-run it each year then no guarantees – we voted we did not want a hybrid system of RBM and bright lines.
- How do we accomplish maintaining what we have and building on it? Shouldn't build on current list?
- Shouldn't lose ground, but not sure how do that
- Started with control centers – how do we address those, keep those in?
- Keep thresholds for data collection to see if they do anything for us
- Recommendation to put off decision until we get the data to analyze?
- Yes, keep thresholds in for data request
- Need data to inform the decision for the final version
- Only have one shot at data collections
- If leave thresholds in here then set false expectation in the industry that smaller units will not need to be covered – acquiesce in doing it, but concerned
- Do we still add criteria to drive data request directed at control centers – one that just says control center to have a baseline to compare to?
- Suggestion for 1.20 – have criteria with a lot of numbers – is that the right number? If number goes down then adjust the criteria – this goes away if we use survey for its purpose.
- Survey does not tell us how to adjust if we do not get the number expected.
- Maintain what you are doing along with the minimum as an interim step
- Also need to pay attention to survey ability to test additional thresholds – to see how the different levels play out and allow us to adjust high and medium
- Would not capture below 2000 MW – we have a hole in the control centers we could identify TS – seems we need more granularity in the survey – still also don't know what the number should be – why are they reluctant to give us a "good" number they are looking for?
- Regions are still developing and do not have the numbers they are trying to establish.
- Possible to get numbers back to review in August?

- Scott Rosenberger suggested using the team members as an initial sample.
- Leverage EEI members to get some numbers? Question number 2 will help but may have multiple assets that cover across categories.
- What we put in the survey will drive industry expectation especially given attachment #1 is our criteria – otherwise Howard will have to respond to comments about why did you choose that level.
- Draft survey already out there for comment.
- Always free to add anything we want to the list
- Aware anything we put out will look like a possible standard – everything is under development until approved – language says looking for data to inform development – cannot prevent them from reading implications into language – need to be sure to state this is not the final product.
- There is a value in its looking different.
- Should the Team file formal comment to allow staff to respond and change?
- Would require a call before Chicago with a quorum which has been difficult to obtain on a call.
- Not putting developing final criteria language off indefinitely, but need data to inform us.
- May be rare opportunity to hold an email vote on this issue of comments to the survey.
- Additional discussion on transmission language?
- Beyond the survey is that a concept we need to capture?
- Requires changes to R2
- Are we good with the concept? We struggled with specific words – capture in concept statement – the "fence theory"

III. CIP 011 SUB-TEAM PROGRESS REPORTS

On Friday morning the Vice Chair asked each Sub-team lead to give a report on progress since the Sacramento meeting. He suggested that as a minimum, each sub-team should complete its summary of industry informal comments received as well as the Dallas workshop input so a response document can be developed and be prepared for posting.

A. Sub-Team Progress Reports

1. Systems Security and Boundary Protection

Members: Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell) (FERC: Justin Kelly)*

Jay Cribb reported on the Sub-team's efforts since Sacramento. They have split up and assigned requirements to member and are making progress – one or two troublesome ones we may recommend deleting, will distribute explanation – working with DJ's team to coordinate on perimeters – putting a straw man for both groups to review.

Member Comments:

- How much more time does your Sub-team need? A: As much as the schedule will allow us – also trying to use terminology from 003-009 to make industry comfortable.

2. **Recovery Management**

*Members:*Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)(FERC: Dan Bogle)*

Scott Rosenberger reported that the Sub-team made some but not substantial progress over the past several weeks.

3. **Personnel and Physical Security**

Members: Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*

Doug Johnson spent time looking at rationale and his sub-team still needs to know if we are splitting the rationale out into one box and guidance into a separate box – still need to look at the levels again and be sure incorporated external communication and connections in proper way – meeting and coordinating with Jay's group – also working to coordinate with Sharon's group on revocation

4. **Change Management, System Lifecycle, Information Protection, Maintenance, and Governance**.

Members: Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)(FERC: Jan Bargen, Matthew Dale)*

David Revill offered a report from the "hodge-podge" sub-team. He noted they had made good progress based on feedback in Sacramento. They have tried to address areas of overlap with other teams. They have also crafted new requirement for vulnerability assessment and believe they are a few side meetings away from presenting to full group.

Have not documented responses to informal comments yet – we need whatever time we can get plus one day.

5. Access Control

Members: Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell) (FERC: Mike Keane)*

Sharon Edwards reported on the sub-team electronic access good meetings. R7 added text boxes – reviewed other changes by requirement: R9 combined with R13, divided revocation into 4 distinct categories, leave of absence, voluntary and involuntary revocation,
R10 – passwords, if used as authenticators – tried to avoid TFEs.

6. Implementation Plan Sub-Team

Members: Scott Mix (Lead), Doug Johnson, John Lim, Jim Brenton, Tom Stevenson, Joe Bucciero, Bradley Yeates, William Gross, *(Jeff Drowley)(FERC: Jan Bargen, Mike Keane)*

This Team will be assisting with the CIP 002-4 implementation plan.

The Vice Chair thanked the sub-teams for the significant work done by sub-teams despite the political sideshow. He noted he had underestimated when the SDT could get back to 010 and 011 which may not be until December. Many in industry will want to know what was said and done at the Dallas workshop as well as the industry's informal comments. We need to decide soon how we want to address and respond to those in the future, but for now we need some closure on summarizing the comments we have received. WE may need a conference call or a webinar to explain why we are moving 002-4 and putting the 010 and 011 on hold. He urged each sub team to hold at least another call in order to create a response summary to industry comment by the Chicago meeting.

Industry Response Format Comments

- Format for that? # and summary of responses?
- Similar to responses last December – highlight of responses.
- Responses by question or free form – do we need a common format?
- Our team cannot respond by question but a common format might be helpful – will template a format for sub teams to use.
- Can say this is what we heard but not formulate how we will address the comment yet.
- Sub teams were provided summaries of comments related to their group – promised the industry we would publish comments from Dallas workshop

- Each group needs to review the transcripts from Dallas
- Spreadsheet from Bryan might be helpful in this process

B. Initial Discussion of CIP 010 and 011 Schedule

In light of the CIP 002-4 effort and the Sub-Team reports the Vice Chair asked the SDT to discuss issues surrounding the development of a revised CIP 010 & 011 schedule. Below are discussion points made.

Member Discussion Points

- Schedule – no end date formally communicated yet.
- Allen Mosher – finish product enacted by Dec 2011.
- What date does team have to deliver product to get approval by Dec. 2011.
- Sooner we get product to industry for comment the better the end product and more opportunity for industry to internalize the implications and build acceptance.
- Only have the schedule that starts ballots in January and ends in July
- Roughly move ballot in summer to end by December
- Try to prepare by May to get more rounds of comments
- Survey is in Word format – encourage team to offer suggestions
- Trying to put in additional criteria to establish useful numbers – should we break the h-m-l and instead put into a series of questions to avoid perception of moving toward a specific standard – allows to test different levels regarding control centers
- Concerned send out draft attachment 1 industry will take that as final product – reformat attachment?
- Just ask twenty-two questions rather than a table? Avoid industry expectation of the standard
- Trying to figure out how we capture the data
- Two different sets of questions
- More efficient to fill out the table?
- It is the h-m-l that will make people associated numbers to the potential standard
- More than twenty questions if ask about medium too
- Reorient the table in question 2
- We will use the results to explain why we changed the criteria numbers
- We are not set up to ask for the right threshold number
- We will know the response to the number of assets under threshold of 2000 and 1000
- Ask for as many pieces as you can to help inform 002-4 development and for 010 and 011 development
- But the more difficult you make it for entities to respond – trying to keep response burden to a minimum but get the most useful information – trying to balance

- Take the same assets from question 1 and now separate out into categories – sum of #2 will equal #1 – question #3 gets to the additional assets from bright lines – do we need a question to capture those assets that drop off
- May have a critical asset that is not even captured in question #1
- Question #3 gets to the delta between what you do today versus what you might do with bright line criteria
- Too complicated to ask questions to get to the right number? Need data to help set the hard break of bright lines
- Generation units we put on because of transmission constraints – but those units will not be identified in this survey
- We did an analysis based on the version 3 that went out in May for comment – ask the question more directly about what assets would be added and ask if items drop out ask why rather than asking for a number and then subtracting to figure out the corresponding numbers – makes information more transparent and will gain greater acceptance in the document
- That becomes more than a data request and would require team responses – team has to take data and respond by making changes to then post document within a week – captures a fine level of detail the team may not have enough time to respond to and reflect in the document to post
- Suggestions will be part of comment responses to the survey
- Sum of question #2 must equal #1 is lost in the middle of the paragraph – should make that more explicit in the directions or bolded
- Have to tell them they have to put items from #1 in one and only one spot in #2
- Any critical assets that cannot be categorized in #2 – we have a category for low
- We ask for anything else – this gets at the assets identified as important but not captured by the risk based assessment
- Can team members take an early run at completing survey as a sample to look at in Chicago
- Won't have final version of the survey ready until July 28 to be posted as part of package to Board of Trustees
- Won't be much advanced notice. Straw survey-
- Get a not quite final form. Fill out and then bring to Chicago. (before beginning)

IV. NEXT STEPS

Phil Huff noted the 002-4 team will continue working. Implementation plan development for 002-4 *(use the CIP 10 and 11 implementation team).* Guidance/ Rationale. Members will try to get their companies to do the survey. The suggestions on framing the survey will be incorporated as discussed by NERC. CIP 10 and 11 sub-teams should capture work done and keep meeting to develop industry comment summary. Phil offered to send out a template for the sub-teams to use. All members should review the transcription of workshop and provide NERC any feedback by Chicago on any red flags or mistakes.

The Vice Chair noted the Detroit open Smart Grid meeting next week. Phil will send out request of other SDT members to see if any can attend and suggested that the SDT would like to continue collaboration but was unlikely for their next meeting.

The SDT will consider going to 3-day meeting schedule after September with longer days on Tuesday –Thursday. The Vice Chair asked members to make the commitment to stay through to Friday noon at the next SDT meeting in Chicago. He also said that in light of the quorum requirements he and the Chair will consider an attendance policy and consult with members who have had difficulty in participating over the past several months. The SDT reviewed the issue of a letter of appreciation to the CEO's of the member companies from the President of NERC for the hard work and commitment of the members to the CIP revisions. It was agreed that NERC staff would take any requests from members to the NERC president.

Finally, the Vice Chair, on behalf of the SDT, thanked Sam Merrill and the CERT for their excellent hosting and facilities. He noted Doug Johnson will be our host in Chicago in August and urged members to register for the session.

Meeting adjourned at 11:30 a.m.

Appendix #1

Project 2008-06 Cyber Security Order 706 SDT

Draft 24th Meeting Agenda

July 13, 2010, Tuesday- 8:00 AM to 5:00 PM EDT

July 14, 2010 Wednesday- 8:00 AM to 5:00 PM EDT

July 15, 2010 Thursday- 8:00 AM to 5:00 PM EDT

July 16, 2010 Friday- 8:00 AM to 12:00 PM EDT

CERT Software Engineering Institute, Carnegie Mellon University

Pittsburgh, PA

NOTE:

1. Agenda Times May be Adjusted as Needed during the Meeting

2. Drafting and Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4
- To explore and clarify the Work Plan and Schedule for completing CIP-010 & 011
- To review, clarify and refine the strawman CIP-002-4 standard proposal
- To convene sub-teams to review the sub-team responses to Industry comments and proposed changes to CIP-010 and 011
- To provide SDT guidance so sub-teams can make further refinements to CIP 002-4, 010 & 011
- To agree on next steps and assignments

Tuesday, July 13, 2010 8:00 a.m. - 5:00 p.m.

- Introduction, welcome, and opening remarks -*(Morning)*
- Overview of CSO706 SDT Work plan and schedule for CIP 002-4 and Explore and Clarify CIP 010 & 011-*(Morning)*
- Review and seek agreement on proposal for refining the SDT Consensus Procedures -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review and refine draft CIP 002-4 standard and related documents. *(Morning)*
- "Lunch and Learn"- Format Proposal*(Lunch)*
- Review and refine draft CIP 002-4 standard and related documents. *(Afternoon Plenary)*

Wednesday, July 14, 2010 8:00 a.m. - 5:00 p.m.

- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Morning Plenary)*
- "Lunch and Learn"- NERC CIP SDT and the ASAP-SG Architecture Team
- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Afternoon Plenary)*

Thursday, July 15, 2010, 8:00 a.m. - 5:00 p.m.

- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Morning)*
- "Lunch and Learn"- Substation Networks (Varnell)

- CIP-010 and 011 Sub-Teams address changes in requirements in light of industry c*omments & i***n**puts from the SDT *(Afternoon)*
- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Afternoon)*

Friday, July 16, 2010, 8:00 a.m. - 12:00 p.m.

- Review of CIP-002-4 Refinements (Morning)
- Review SDT Workplan Schedule to prepare new Draft CIP-010 and 011 Requirements documents. *(Morning)*
- Review Next Steps and Sub-Team schedule and SDT Chicago Meeting Agenda (*Late Morning)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT DRAFTING SUB-TEAMS (JULY, 2010)

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
Implementation Plan	Scott Mix (Lead), Doug Johnson, John Lim, Jim Brenton, Tom Stevenson, Joe Bucciero *(Nuclear: Bradley (Brad) Yeates, William Gross, Jeff Drowley)* *(FERC: Jan Bargen, Mike Keane)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 25th Meeting Agenda
August 10, 2010, Tuesday- 8:00 AM to 5:00 PM CDT
August 11, 2010 Wednesday- 8:00 AM to 5:00 PM CDT
August 12, 2010 Thursday- 8:00 AM to 5:00 PM CDT
August 13, 2010 Friday- 8:00 AM to 12:00 PM CDT
Exelon Corporation
10 S. Dearborn Street, 48th Floor , Chicago, IL
NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the adopted CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4 in 2010
- To review and adopt a Work Plan and Schedule for completing CIP-010 & 011 in 2011
- To review and discuss the results and implications of SDT member companies' data survey results for the CIP 002-4 draft.
- To review, clarify, refine and adopt CIP-002-4 standard proposal for NERC staff review
- To review CIP-010 & 011 sub-teams draft responses to industry and Dallas workshop
- To agree on next steps and assignments

Tuesday, August 10, 2010 8:00 a.m. - 5:00 p.m.

- Introduction, welcome, and opening and guest remarks -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review of CSO706 SDT Work plan and schedule for CIP 002-4 *(Morning)*
- Review of CSO706 Draft SDT Work plan and schedule for CIP 010 & 011 *(Morning)*
- "Lunch and Learn"- Forensics U.S. CERT *(Lunch)*
- Overview of NERC Survey Development and Industry Comments *(Afternoon)*
- Review and refine draft CIP 002-4 standard and related documents *(Afternoon)*

Wednesday, August 11, 2010 8:00 a.m. -5:00 p.m.

- Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting *(Morning)*
- Review and refinement of CIP-002-4 documents including implementation plan for NERC staff review *(Afternoon)*

Thursday, August 12, 2010, 8:00 a.m. - 5:00 p.m.

- Adoption of CIP 002-4 documents for NERC staff review *(Morning)*
- Adoption of CIP 010 & 011 Draft Schedule *(Morning)*
- CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input *(Morning and Afternoon)*
- Agree on schedule for incorporating draft responses to Industry Comments and Workshop input into a single response document. *(Afternoon)*

Friday, August 13, 2010, 8:00 a.m. - 12:00 p.m.

- Review directions and next steps to CIP-010 and 011 Sub-teams – *as needed (Morning)*
- Address 002-4 planning for September Webinar *(Morning)*
- Review SDT September 8-10, 2010 Winnipeg Meeting Agenda (*Late Morning)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706 SDT
Draft 25th Meeting Agenda
August 10, 2010, Tuesday- 8:00 AM to 5:00 PM CDT
August 11, 2010 Wednesday- 8:00 AM to 5:00 PM CDT
August 12, 2010 Thursday- 8:00 AM to 5:00 PM CDT
August 13, 2010 Friday- 8:00 AM to 12:00 PM CDT
Exelon Corporation, Chicago, IL
NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the adopted CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4 in 2010
- To review and adopt a Work Plan and Schedule for completing CIP-010 & 011 in 2011
- To review and discuss the results and implications of SDT member companies' data survey results for the CIP 002-4 draft.
- To review, clarify, refine and adopt CIP-002-4 standard proposal for NERC staff review
- To review CIP-010 & 011 sub-teams draft responses to industry and Dallas workshop
- To agree on next steps and assignments

Draft Agenda

Tuesday	**August 10, 2010 - 8:00 a.m. - 5:00 p.m.**
8:00 a.m.	Welcome and opening remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines- *Joe Bucciero* Facilitator review and SDT acceptance of July 13-16, 2010 Pittsburgh SDT meeting summary
8:15	Review of meeting objectives, agenda and meeting guidelines- *Bob Jones*
8:20	Standards Committee Chair and Senior NERC Management Comments to the SDT on their work
8:40	Review of CSO 706 SDT CIP 002-4 adopted work plan and schedule: *Stu Langton*
8:45	Review and Discussion of CSO 706 SDT CIP 010 & 011 draft work plan and schedule: *Stu Langton*
9:30	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
10:00	*Break*
10:15	Overview of SDT CIP 002-4 Strawman documents
10:45	Review and refine draft CIP 002-4 standard and related documents
12:00	"Lunch and Learn"- Forensics U.S. CERT *(Lunch)*
1:30	Overview of NERC Survey development and industry comments
2:00	Review and refine draft CIP 002-4 standard and related documents
3:15	*Break*
3:30	Review and refine draft CIP 002-4 standard and related documents
4:50	Review any drafting assignments and Wednesday agenda
5:00	*Recess*

- *Possible Ad Hoc Drafting or Sub Team Meetings- Evening*

Wednesday	**August 11, 2010 - 8:00 a.m. - 5:00 p.m.**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:15	Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting
10:00	*Break*
10:15	Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting
12:00	*Lunch*
1:00	Review and refinement of CIP-002-4 documents including implementation plan for NERC staff review
3:00	*Break*
3:15	Review and refinement and consensus testing of CIP-002-4 documents including implementation plan for NERC staff review
4:50	Review any drafting assignments and Thursday agenda
5:00	*Recess*

- *Possible Ad Hoc Drafting or Sub Team Meetings- Evening*

Thursday	**August 12, 2010 - 8:00 a.m. - 5:00 p.m.**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *Phil Huff, Joe Bucciero*
8:15	Adoption of CIP 002-4 documents for NERC staff review
9:00	Review and Adoption of CIP 010 & 011 Draft Schedule
10:00	*Break*
10:15	CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input
12:00	*Lunch*
1:00	CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input
3:00	*Break*
4:30	Agree on schedule for incorporating draft responses to Industry Comments and Workshop input into a single response document *(Afternoon)*
4:50	Review any drafting assignments and Friday agenda
5:00	*Recess*

- *Possible Ad Hoc Drafting or Sub Team Meetings- Evening*

Friday	**August 13, 2010 - 8:00 a.m. - 12:00 p.m.**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *Phil Huff, Joe Bucciero*
8:15	Address CIP 002-4 schedule and tasks including planning for September Webinar
10:00	*Break*

10:15	Review directions and next steps to CIP-010 and 011 Sub-teams
11:00	Review CIP-010 and 011 Sub-Team Schedule
11:30	Review the Winnipeg Meeting Agenda and Next Steps and Assignments
12:00	*Adjourn & Lunch*

- **Appendix # 2 Attendees List**

July 13-16, 2010, Pittsburgh PA

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (T/W)
2. Jim Brenton	ERCOT
3. Jay S. Cribb	Southern Company Services
4.Jackie Collett	Manitoba Hydro (W/Th/F)
5.Joe Doetzl	Kansas City Pwr. & Light Co (T/W/Th)
6. Sharon Edwards	Duke Energy (T/W/Th)
7.Gerald S. Freese	America Electric Pwr.
8. Jeff Hoffman	U.S. Bureau of Reclamation, Denver (T/W/Th)
9. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
10. Doug Johnson	Exelon Corporation – Commonwealth Edison
11.Rich Kinas	Orlando Utilities Commission (T/W/Th)
12. Patricio Leon	Southern California Edison
13. John Lim, Chair	Consolidated Edison Co. NY (T/W)
14. David Norton	Entergy (T/W)
15. David S. Revill	Georgia Transmission Corporation
16. Scott Rosenberger	Luminant Energy
17. Kevin Sherlin	Sacramento Municipal Utility District (T/W/Th)
18.Tom Stevenson	Constellation
19. John Van Boxtel	WECC (T/W/Th)
Scott Mix	NERC
Roger Lampila	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

19. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Members Not Participating

Frank Kim	Hydro One Networks Inc. (Th/F)
Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
Jonathan Stanford	Bonneville Power Administration
William Winters	Arizona Public Service, Inc.

Others Attending in Person

Jan Bargen	FERC
Summer Esquerre	NextEraEnergy (FPL)
Jim Fletcher	American Electric Power
Michael Keane	FERC
Drew Kittey	FERC
Jason Marshall	Midwest ISO
Sam Merrell	CERT/Software Engineering Institute
Brian Newell	American Electric Power
Anna Wang	Burns & McDonnell

Brian Newell - AEP
-
Robert Preston Lloyd - SCE
Alex Salinas - SCE
Sam Merrell - SEI/CERT
Jim Stevens - SEI/CERT

Others Attending via Readytalk and Phone
July 13, 2010, Tuesday
July 14, 2010, Wednesday
July 15, 2010, Thursday
July 16, 2010, Friday

Appendix #3 NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

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

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subgroups) may have a negative impact on particular entities and thus in that sense

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

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

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

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

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

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

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

Any other matters that do not clearly fall within these guidelines should be reviewed

with NERC's General Counsel before being discussed.

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
OPTIONS 1 AND 2

Appendix X
CIP VERSION 4 PARKING LOT (JUNE, 2010)

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
Review clarity of item 1.1, Attachment 2 – Generation Facilities and criteria for Contingency Reserve and Reserve Sharing	Rich Kinas	4/29	CIP-002	**AI:** Revise item 1.1 with input from the industry through the informal comments received.
Shouldn't there be delegations made by the Senior Manager for any exceptions (CIP-011 R2 & R3)	Jackie Collett	4/29	Governance	**Resolved** by the revised CIP-011 text that was posted.
User type access (R3) 3.2 Review the need for network device training (Operators, etc.)	Jim Brenton	4/29	Physical/Cyber & Access Control	Possibly regarding the level of access for outward facing and inward facing devices. What type of user training is required for each level? **Add role-based access (e.g., admin vs. application level access) – physical access & training requirements. Awareness training for everyone, and role-based training as required.**
Combine tables for electronic and physical access control systems (R6, R20, & R22)	Philip Huff	4/29	Physical and System Security	**AI:** Double-check that the proper requirements are incorporated in the respective tables.
Remove ~~Training~~ Termination for physical	Doug	4/29	Physical	

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
access to Low Impact (R9)	Johnson			
What do the blank cells mean in the tables in instances where a timeframe is given? (R9)	Jackie Collette	4/29	Howard Gugel	Do they mean there is no requirement at that particular level? **AI:** Double-check the table entries to ensure that the entries are indicative of the requirement. Possibly a statement should be added to the Guidance Document that describes what is meant by a blank entry in a table.
Monitoring the baseline configuration means monitoring the physical location as written. (R23)	Rob Antonishen	4/29	Change Management (Dave Revill)	**AI:** Is baseline the right term? What do we mean by changing physical location?
What timeframe for issuing alerts (Table entry 18.2)	Jackie Collett	4/29	System Security	**AI:** What is the response time requirement? In what timeframe should the alerts be issued?
Need to address what disciplinary actions are? Should physical or cyber access be revoked?	Jackie Collett	5/11	Disciplinary actions (physical/cyber access)	AI:
Combine the revocation of physical and electronic access requirements (including remote access) into one topical area of the standard	Phil Huff	5/11/2010	Personnel access (Sharon Edwards)	**AI:** Need to investigate possible alternatives. Have a requirement to develop a procedure for handling

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
				revocation of access.
Review "objective" statements to ensure they do not implicate requirements	FERC	5/27/2010	All	
Make requirements text consistent throughout the Standard	FERC	5/27/2010	All	
Global review of adjectives like "sufficient", "appropriate", etc.	FERC	5/27/2010	All	
Baseline for Low level of Impact	Drafting Teams	6/10/2010	ALL	**Completed on 6/10/2010**
Description of Timing (e.g., annual, months, etc.)	Howard	6/10/2010	NERC	
Protection requirements for electronic and physical access control systems	Doug/Phil	6/10/2010	ALL	
Broad Application of TFE Statement	SDT	6/9/2010	ALL	
Gantt Chart for Compliance Deadlines	Varnell	6/9/2010	Howard	
Exclusion for Entities that don't own cyber systems	Doug	6/10/2010	Full SDT	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #5 SDT Consensus Procedures
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
Proposed Refined Consensus Guidelines (May, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least ~~75%~~ 2/3rds favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing a Team consensus on substantive issues ~~which the industry will need to approve by a 2/3's vote.~~

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 (18 members) of the 26 appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).
2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the Team's adopted procedural guidelines, to make and approve formal motions. However, the 2/3rds super-majority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

Appendix #
CSO 706 SDT DRAFTING SUB-TEAMS AND PRINCIPLES

Sub-Team	
CIP 010 (002-4) BES System Categorization	John Lim, Rich Kinas, Jim Brenton, Jackie Collett, *Bill Winters*, Dave Norton, *Jay Cribb* *Rod Hardiman (Observer)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell John Van Boxtel, Jackie Collett, Phil Huff
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson, (*Observer Participants: Jason Marshall*
Access Control	Sharon Edwards (Lead), Gerry Freese, Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Governance, Change Management, System Lifecycle and Information Protection and Maintenance	Dave Revill (Lead), Keith Stouffer, Bill Winters, Jon Stanford, Phil Huff *Observer Participants: John Fridye*