NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Notes
## Cyber Security Order 706 SDT — Project 2008-06

August 10, 2010 | 8 AM to 5 PM CDT
August 11, 2010 | 8 AM to 5 PM CDT
August 12, 2010 | 8 AM to 5 PM CDT
August 13, 2010 |8 AM to 12 PM CDT
Chicago, Illinois

**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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

## CSO706 SDT August 10-13, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Cyber Security Order 706 SDT- Project 2008-06**
**25TH MEETING**
**August 10-13, 2010**
**Chicago, IL**

# EXECUTIVE SUMMARY

On Tuesday morning, John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Chicago and thanked Doug Johnson for hosting the meeting. Doug reviewed the logistics for the meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero also reviewed the need to comply with NERC's Antitrust Guidelines each day of the meeting, and reminded all participants that the meeting has been publicly noticed and is open to the public. John Lim reviewed the proposed meeting objectives and agenda.

On Thursday morning, the SDT unanimously adopted the July 13-16 Pittsburgh meeting summary with edits presented by John Van Boxtel.

The Chair noted the opportunity of the SDT to hear from Allen Mosher, Chair of the NERC Standards Committee on the SDT's efforts and progress. Allen Mosher addressed the SDT noting the atypical external pressures on the Team related to the nature of the CIP changes the Team has been charged to develop and the level of scrutiny due to the high degree of interest in Washington among agencies and congress in cyber security. He urged the SDT to preserve the two-track approach to developing the CIP standards noting this is an important opportunity to prove to political and regulatory interests that the industry can produce effective cyber security standards and do it promptly. Completing the CIP 002-4 process by the end of this year will help demonstrate to Congress that the industry is capable of self-regulation. Mr. Mosher reiterated that he believed that CIP-010 and CIP-011were the right model, and he hoped the SDT would be focusing again soon on that task. He acknowledged that the CIP 002-4 approach was not a risk based assessment, but stressed the importance of analyzing the data rewquest results regarding "bright lines" to determine whether there will be an increased number of CAs and CCAs. At the end of the day on Tuesday, Allen Mosher thanked the SDT for what it is doing in working as a drafting team to develop consensus. He suggested the SDT is making significant progress on something that is very hard to do.

On Thursday morning, John Lim introduced Herb Schrayshuen, the new NERC Vice President and Director of Standards, who joined the SDT meeting on Thursday morning. He thanked each member for their service and understood and welcomed their questions, recognizing the tensions in the process and feelings about how the SDT has been treated over the past couple months. He took questions from SDT members on: what is success for CIP 002-4; system vs. assets approaches; physical security; and the present culture of

compliance and standards. He noted that process is important but so is delivery. Responding to a question of what success looks like for the SDT's work, he suggested that a standard that helps the industry deal with deficiencies in the current standards and delivers results that improve the cyber security framework of the grid could be characterized as success. He promised to help the SDT secure the necessary resources and assistance to get their job done successfully. The culture of compliance versus the culture of reliability is an on-going debate on how to approach cyber security. He noted that we cannot comply our way to reliability. Mr. Schrayshuen noted that NERC will soon release a new reliability standards approach, including how to prioritize the work to be accomplished.

On Wednesday morning, NERC staff (Howard Gugel) reviewed with the SDT the industry's comments and the NERC responses and changes on the draft NERC Data Request. Howard also presented a summary of the inputs received from the six entities that volunteered, as SDT members, to provide an early unofficial response to the Data Request. This very small sample of inputs included data from some large and small entities. Although this represented a very insignificant sampling as a statistical analysis, it did show a net gain in the number of assets being classified as critical. No one entity showed fewer assets as critical by using the bright line criteria included in the draft Data Request.

On Tuesday morning, John Lim provided an overview of the work by the CIP-002-4 sub-team in refining the CIP 002-4 draft taking into account the inputs received during the Pittsburgh meeting. He noted that following its review and refinement at the Chicago meeting, the SDT will seek to adopt the revised draft CIP-002-4 standard and provide a draft to NERC staff for their review and proposed edits. In Winnipeg, the SDT will review and analyze industry's responses to the NERC Data Request, review NERC staff edits to the draft CIP 002-4 standard text, and review and refine several associated documents including: an implementation plan, a guidance document (including rationales for Attachment 1 criteria), and a summary of industry informal comments on CIP 010 Attachment 2 from which CIP-002-4 Attachment 1 is drawn.

The SDT reviewed and refined each section of the draft CIP 002-4 standard text, and as needed, conducted straw polls on the acceptability of the proposed language. The SDT reviewed, refined, and tested the criteria listed in Attachment 1 of the draft CIP-002-4 standard text, which was prepared in advance of the Chicago meeting. On Thursday morning the SDT unanimously adopted the draft CIP-002-4 standard text as revised for review by NERC staff before the Winnipeg session.

NERC staff (Scott Mix) presented a proposed approach for the CIP-002-4 Implementation Plan to the SDT, which is based on utilizing the currently FERC approved CIP V3 "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities" document. Since the SDT isn't making any significant changes to the CIP-003 through CIP-009 standards, the only significant addition would be to determine the

implementation for CIP-002-4, which was proposed as the start of the first quarter following FERC approval. Based on the assumptions discussed in the meeting, the starting date for this plan would be July 1, 2011.

This approach was presented to the SDT at the Pittsburgh meeting and then refined based on that discussion. Scott noted that the schedule assumes a FERC order on the last day of a calendar quarter, and therefore the proposed schedule is aggressive, but achievable, and probably meets FERC's expectations. He suggested that a 24-month implementation schedule in all cases would likely not be acceptable to FERC based on past experience. The Chair suggested that following the review and testing of alternative approaches he would look to forming a drafting sub-team to develop a proposed implementation plan for review and adoption in Winnipeg. (See Appendix #7 for the full set of discussion notes).

SDT Member and participant discussion comments on the proposed implementation plan approach touched on: the importance of a communication plan to the industry; the possibilities for FERC approval of the plan; the impact of bright lines on implementation timing questions; the ability to budget for these changes in a timely manner; whether the NERC Data Request information will help guide the implementation plan draft; and the implementation timing regarding nuclear generation facilities.

Following the discussion of the proposed approach, a revised implementation plan concept statement was presented by Scott Mix. The discussion of the revised implementation concept included: clarifying its approach as covering the one time exemption/override for 24 months for newly identified CCAs at newly identified CAs but with all other requirements being consistent with the currently approved implementation plan; factoring in Order 706B requirements and the timing requirements for filing TFEs; and clarifying how this implementation plan would impact or be impacted by the new Urgent Action SAR on CIP 005 that is being drafted. A straw poll on the acceptability of this implementation plan concept did not gain a supermajority of support (2/3s) from the SDT.

Following the straw poll the SDT identified and discussed the following potential alternative approaches:

a. Implementation plan would require identification of CAs within 1 quarter and CCAs within 4 quarters of its approval. Existing Newly Identified CCA Plan could be used, but the clock would not start for these new CCAs until 4 quarters (12 months) after approval
b. Develop a new implementation plan that allows:
    1. 24 months for implementation of Newly Identified CCAs at New CAs and
    2. Uses the existing implementation plan criteria for the Newly Identified CCAs for New CCAs at existing CAs

c. Keep the existing Newly Identified CCA Implementation Plan but add one quarter to Scott Mix's original plan for the effective date

d. Develop a one-shot/one time exception of 18 months (for specific circumstances) with a sunset to the existing implementation plan schedule
e. Provide six months to identify new CCAs and 24 months to implement compliance for the Newly Identified CCAs.

SDT Member and participant discussion of the potential alternatives included: clarifying the impact and pros and cons of each alternative approach in terms of the possibility of delaying FERC's approval; the observation that the issues affect mostly generation with some transmission; considering these options from an audit enforcement perspective; the visibility of a clear date for compliance is critical to show movement forward on implementation; and less effort to justify changes if tied to the already FERC approved implementation plan. The consensus was that the SDT had reached general agreement on the implementation plan concepts, but hadn't settled on the length of time allowed for compliance. Building on this discussion, the following revised concept was presented:

- For the initial application of the "bright lines" in CIP 002-4, CCAs at newly identified CAs will be compliant at 24 months from identification (includes 706B items and TFEs)

- By the effective date of the CIP-002-4 standard (the first day of the second full calendar quarter after regulatory approval), the registered entity will need to identify its CAs and CCAs and has xx months from that date to be compliant with CIP-003 through CIP-009

- For subsequent application of the "bright lines" in CIP-002-4, CCAs at newly identified CAs will be compliant according to the existing Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

- For all implementations of Newly Identified CCAs at existing CAs, the existing Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities will apply as it currently exists.

The Chair and Vice Chair suggested that there was now enough input for a drafting sub-team to prepare a new implementation plan proposal, and volunteers for a drafting sub-team were solicited to develop a plan and bring it back for the SDT's consideration in September. The following members agreed to join the implementation plan drafting sub-team: Sharon Edwards, Phil Huff, Dave Norton, Dave Revill, Scott Rosenberg, and Kevin Sherlin. Mike Keane (FERC) and Scott Mix also asked to participate. Joe Bucciero will facilitate the discussions.

On Tuesday morning, Phil Huff presented a draft project schedule for CIP-010 and CIP-011, which had been circulated to the SDT prior to the meeting, and asked Allen Mosher to provide the Team with any preliminary feedback prior to its fuller discussion and proposed adoption on Thursday. Phil reviewed the draft project schedule that includes a

posting for 45-day formal comment period in late May 2011 and with no informal postings between January and May anticipated. This approach is based on the SDT's experience and feedback from industry earlier this year with CIP-010 & CIP-011. Mr. Mosher suggested the SDT may still want to consider an informal comment period. The Chair noted the SDT's hope and expectation is that if NERC can develop a good communication plan, it can help prevent or minimize the industry's confusion and reduce the anxieties as well as allow for some informal feedback. The SDT will be focused on providing clear requirements for the standards, along with an explanation of the rationale, and build on multiple rounds of formal comment. The draft schedule proposes three rounds of comment and balloting.

On Thursday afternoon, the SDT took up the review of the schedule and tasks for completing its work on the CIP 010 & 011 standards. There was an extended SDT member and participant discussion that covered three broad issues: agreeing on the SDT schedule; preliminary work on next phase; and a deeper issue of the approach to drafting during the next phase.

The discussion on Thursday afternoon covered the following topics: schedule; industry confusion vs. communication; clarification of SDT deliverables- short and long term; sub-team role in setting out proposed approach for full SDT review; SDT organization and management in 2011; clarification of the SDT's overall approach to CIP and validating the work to date; the role of security and costs in designing the CIP standards approach; clarification of FERC's direction to the SDT; clarification of the problem the SDT is addressing- including reviewing the original SAR; NERC's investment and expectations of the SDT in getting the job done; conflicting industry and regulator expectations; and the need for a high level of communication with the industry in 2010 and 2011.

On Friday morning, John Lim reminded SDT members of the importance of working together as a team. Phil Huff offered two new motions describing a process for moving forward on foundational concepts based on Thursday's discussion. The first motion was approved by a voted of 16-1, and the second motion was unanimously approved by a vote of 17-0.

1. The CSO706 SDT will prepare a complete package for initial posting to the industry for consideration and ballot in July 2011, in response to FERC Order 706, with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without major redirection of SDT efforts.

2. The CSO706 SDT will form a sub-team to develop a framework for presenting and scoping cyber security requirements for preliminary delivery in October 2010 and completion in December 2010. This deliverable would include the form of the standards and the basis by which the requirements are written and applied. The output of this team would go before the full SDT for review and

approval. This task would not include the actual development of security requirements.

The Chair asked for volunteers for the Framework Sub-Team and the following members responded: Dave Norton (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. In addition, Mike Keane and Scott Mix will join and Joe Bucciero will serve as facilitator. It was agreed that Joe Bucciero would send a note to those members of the SDT not present asking for others who might want to volunteer.

Following the vote, the SDT agreed on the following direction to the current CIP-011 Sub-Teams: the sub-teams need to prepare and finalize the responses to industry comments on CIP-010 & CIP-011 as well as the workshop comment summaries so these documents can be posted in October and recognize industry's investment into those comments.

On Friday, Scott Mix provided an overview of the CIP 005 Urgent Action SAR and the process to date. He urged individual members to provide their comments when the SAR is posted and raise issues they discussed at this meeting.

The Chair and Vice Chair discussed with the SDT the Winnipeg agenda that will start on Wednesday morning, September 8 through mid-morning Friday, September 10. The meeting will include the final adoption by the SDT for posting of CIP-002-4, a review of the NERC Data Request results to determine whether any criteria need changes, review of a CIP 002-4 comment response document drawn from the relevant comments on Attachment 2 of the CIP-010 informal posting, and preparation for the September 23 webinar. Brian Newell has offered to create a database that the SDT can use to calculate Data Request question totals. This will be sent around for the SDT to review in advance of the Winnipeg meeting. Herb Schrayshuen, NERC, noted the discussion of whether additional project management service is needed. The Chair suggested that the SDT develop a better clarification of scope for CIP 010 and 011 after December, 2010 discussions of the Framework sub-team and that a review for such a requirement be made at that time.

The Chair asked Joe Bucciero to send out a recurring meeting invitation to put on everyone's schedule for four hours during the fourth week of each month. The first session will be scheduled for Thursday, August 26, from 12-4 p.m., Eastern time. The Chair and Vice Chair thanked Doug Johnson for the excellent hosting and accommodations, especially the Blue Angels demonstration.

*Meeting adjourned at 11:15 a.m.*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# 25TH DRAFT MEETING SUMMARY
**Cyber Security Order 706 SDT- Project 2008-06**
**Chicago, IL**
**August 10-13, 2010**

## I. AGENDA REVIEW, UPDATES, WORKPLAN, SCHEDULE AND REVIEW OF NERC DATA REQUEST

### A. Agenda Review and Meeting Logistics

John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Chicago and thanked Doug Johnson for hosting the meeting who reviewed the logistics for the meeting. Joe Bucciero conducted a roll call (See Appendix #2) and reviewed the antitrust and public meeting guidelines (See Appendix #3) with the meeting participants. On Thursday morning, the SDT unanimously adopted the July 13-16 meeting summary with edits presented by John Van Boxtel. The Chair announced that Frank Kim has resigned from the SDT for professional and personal reasons but will follow the SDT progress and contribute comments where possible. This means that there are 25 SDT members resulting in a quorum rule of 17 members to conduct business. The meeting began with a quorum 17 members in the room and 2 members participating by phone/ready talk.

John Lim reviewed the proposed meeting objectives noting the following three outcomes needed at this meeting: 1. Adopt draft CIP 002-4 – everyone agreeing with language and criteria and utilizing the data request responses of some of the member companies as a guide; 2. Agree on a schedule for CIP 010 and 011 to deliver to the Standards Committee; and 3. review the Sub-team summaries of informal comments and the workshop input. The facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda.

The Chair noted the opportunity of the SDT to hear from Allen Mosher, Chair of the Standards Committee on the SDT's efforts and progress.

### B. Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

Scott Mix provided the SDT an update on the urgent action CIP 005 SAR. Once the Standards Committee approves then it will go out to ballot for SDT formation. The proposed revisions may land about the same time as this groups work on CIP 002. It may be helpful to post together or at the same time. The intention is to include a compliance guidance document that is still being developed with input from companies of differing levels. They are still putting together the SAR

*Member Comments*

- I would like this group to have a look at this before it is pushed through – within the rules but think this group should look at it.
- When is the CAN is issued? When is it guidance versus compliance? It seems multiple people are now writing requirements.
- Allan Mosher noted that compliance is written by NERC staff, reviewed with regions and others – it is compliance guidance to regional staff for understanding for compliance purposes. The Standards Committee is working on setting up a one-stop shop for interpreting standards though interpretations could still be formal or informal.
- This seems like a back door approach to compliance requirements.
- Response to unofficial request for interpretation that was pulled without interpretation – I will submit request in the near future – need formal guidance.
- The CAN process is causing concerns for the industry as a whole. Even if it provides guidance for auditors, it seems that it adds requirements not necessarily in the standard.
- The new SAR seems closely related to our activities.
- There is a different definition of "critical." NERC needs a methodology for what is most critical for reliability – not sure what the background is for that SAR.
- Note that regional entities do not own "assets."
- If it is "critical" it needs to be uniform across industry with a common list. Industry would support unifying such a list to limit confusion and number of compliance officers.
- Unlikely that industry would support lining up critical assets with critical facilities at this point.

Keith Stouffer reported that latest version of the NISTER report was released last week for review. The person leading that effort has moved to FERC. Dave Norton noted that a recent report of insider incidents showed that they were up 28% last year.

### C. Standards Committee Chair Comments to the SDT

Allen Mosher addressed the SDT noting the atypical external pressures on the Team related to the nature of the CIP changes the Team has been charged to develop and the level of scrutiny due to the high degree of interest in Washington among agencies and congress in Cyber security. He noted the industry's high level of concern regarding compliance issues as NERC is in the midst of trying to revamp its compliance system and culture.

He urged the SDT to preserve the two-track approach to developing the CIP standards noting this is an important opportunity to prove to political and regulatory interests that the industry can produce effective cyber security standards and do it promptly. Completing the CIP 002-4 process by end of this year will help demonstrate to Congress that the industry

capable of self-regulation. There is no dispute about the need for a higher degree of regulation of cyber security or statutory authority, though some still question how far that authority should go. By being successful on CIP 002-4 we can take some of the wind out of the sails of those arguing to simply drop the NIST into the CIP security standards. This would cost industry billions of dollars without a guarantee of better security for the grid. We need to provide an effective industry developed alternative or the continued deference to industry self-regulation in terms of NERC's standards process will be in question. If we fail here, it may mean loss of authority in other areas – cyber security is just the initial test.

*SDT Member Questions:*

Members expressed frustration with the SDT's re-direction on CIP 002-4 noting that a political problem has been assigned to a technical group to solve. There was discussion of the perception of some in the industry and those observing this effort that political drivers have resulted in a deadline to identify more critical assets but that CIP 002-4 is not enough.

Mr. Mosher reiterated that he believed that CIP 010 and 011were the right model and he hoped the SDT would be focusing soon on that task. He acknowledged the CIP 002-4 approach was not a risk based assessment, but stressed the importance of analyzing the results of the data request regarding "bright lines" in September to determine whether there will be an increased number of CAs and CCAs. He also acknowledged SDT and industry concerns about creating a workable transition to CIP-010 and 011 and the concerns with compliance and auditing confusion with multiple CIP versions in play. The SDT also discussed that for cyber security the size of the asset may not be the controlling factor. There was also acknowledgement of the need for uniformity of an industry approach. Finally a phase-in period for a risk-based system anticipated by CIP 010 and 011 should be developed to allow the industry to get controls in place.

Mr. Mosher noted his target and focus is on the CIP 010 and 011. He noted that the industry needs an interim step to fix the most egregious gaps in identifying assets in current CIP system but it does not make sense for the SDT to stop at 002-4. The hope is the NERC Data Request results will help guide the team in determining what percentage of increased assets is the right amount or target. It was noted that NERC President Gerry Cauley stated that success in the short term for the SDT would be that industry adopts bright line criteria that can be technically supported. Technical justification for each bright line will be an important part of the SDT discussions going forward vs. the exact number of CAs.

In the last meeting the SDT adopted plan to complete 002-4 as soon as possible and no later than December in order to get back to work of CIP 010-011 development.

At the end of the day on Tuesday, Allan Mosher thanked the SDT for what it is doing in working as a drafting team to develop consensus. He suggested it is making significant progress on something that is very hard to do. He urged them not to fix it for a member's sector or company, but for the industry as a whole, i.e. a set of criteria driven by reliability

that you can justify with engineering. He acknowledged the heartburn on CIP 002-4, but suggested it will make it easier for the SDT to do CIP 010 and 011. Many in the industry are concerned about the big jump to the latter. However, it is the path we are on and you can make it work by explaining why we are doing it and advocating for its adoption.

### D. NERC Vice President and Director of Standards Comments to the SDT

John Lim introduced Herb Schrayshuen, the new NERC Vice President and Director of Standards, who joined the SDT on Thursday morning. He thanked each member for their service and understood and welcomed their questions, recognizing the tensions in the process and feelings about how the SDT has been treated over the past couple months. He noted that process is important but so is delivery. Responding to a question of what success looks like for the work of SDT, he suggested a standard that helps the industry deal with deficiencies in the current standards and delivers results that improve the cyber security posture for the grid. He promised to help the Team secure the necessary resources and assistance and help them get their job done successfully. In response to a question of whether there was some number required to be covered in terms of critical assets under CIP 002-4, Mr. Schrayshuen suggested that the NERC Data Request results will provide some guidance but that there will need to be a technological basis for number of assets covered. He urged the SDT to keep in mind the industry frame within which they are working and the reality that the SDT is going to get more "help" than you may want and that the SDT is on a pragmatic schedule spurred by industry input, although not an ideal schedule from the SDT perspective.

He noted that some members of the SDT have superior knowledge in terms of security clearances and may have concerns about what security approaches work and don't work, e.g. data on frequency issue. This may create an uneven base of knowledge which impedes progress on problem solving. On another SDT, the dynamic within the team led to failure at the ballot. Issues were voiced in drafting team process but not resolved so members left the Team prepared to vote no in the ballot. The drafting team had thought their job was done by simply voicing concerns and then expressing opinions to the industry and voting no on the resulting proposed standard. The lesson is that it is a breakdown of the process for a team not take an issue and try to resolve it here, and when all is said an done, make a team decision informed by this problem solving.

The culture of compliance versus culture of reliability is an important debate on how to approach cyber security. He noted that we cannot comply our way to reliability. Quality control plan training has started and we are looking for conflicts between standards. My last job was compliance manager and I got a zero finding showing it can be done. Experience with the audit process should influence results but not at the expense of lowering the bar. The SDT should try to use it to inform and improve standards.

Mr. Schrayshuen noted that NERC will soon release a new standards approach, including how to prioritize. We are trying to put everyone in the same room, including FERC, to create one list of priorities moving forward in an effort to avoid redirects.

*Member Comments on the SDT's Challenges*

- **What is success for CIP 002-4?** We were on a process to deliver broad coverage, when the team was redirected to a bright line criteria –with a challenge to deliver by end of this year something that the industry must support and regulators have to see as a real "improvement." Do we have a certain number of assets identified to equal "success"?
- Taking your position at an interesting point – this is a whole new thing and responding in an atmosphere of fear – trying to address 100 years of effort with new threats – cyber security overlay with two parts for generation and for transmission worlds resulting in a complex puzzle. Mr. Schrayshuen noted he understand distinctions between them.
- Industry in better shape now from standards and compliance. However, standards Committee and CCC don't have substantive expertise on cyber issues. Also need better subject matter quality control on auditor hires.
- **System vs. Assets Approaches.** The SDT has struggled with two different approaches: a systems focus versus an assets and sites focus. In essence, by analogy, we are being asked to say which airports are the most important vs. protecting the air traffic control system. Mr. Schrayshuen noted he favors an incremental progress to improvement – don't go for "the bridge too far" but don't preclude improved approaches in the future. There may be a need to prioritize in terms of timing – not everything can be important at the same time – build toward a better long term approach.
- Size matters for impact optics, but vulnerability can come from smaller venues.
- **Physical Security.** We are hearing that many are interested in physical security and concerns about how that issue can rearrange priorities. Physical securities over the next five years. That is not within scope. Prioritization is predicated by someone writing a SAR. Since no SAR has been submitted yet on physical security, we cannot assess priority.
- **Culture of Compliance and Standards.** There is a disconnect between standards writing and the nits of compliance. The latter doesn't add security but it does add huge expense. We have to worry about how an auditor will interpret, rather than focus on most reasonable interpretations, (e.g. antivirus on a switch when there has never been a virus on a switch because auditors are asking for it).
- There is growing unrest in the industry about compliance which will need to be addressed sooner rather than later. Inconsistency between regions is one aspect. FERC participation in audits is new as well. The industry looks to requirements as the yardstick, but now having to look at things from FERC that may not yet be in the

requirements. It is increasingly hard to figure out what the yardstick is for measuring compliance.

- Auditing process needs to be better coordinated – need to know the limits, auditors can go anywhere and we can't standardize our compliance programs
- Compliance with TFE process is not equal to the return of effort – cited for insufficient senior manager designation – that is not helpful.
- Many SDT members have gone through audits during the drafting process and they return with a heightened concern about the wording of standards.
- No matter what words are used in the standards, compliance agonizes over the words rather than the intent – examples of the absurd and the pain level and frustration of industry is immense –
- Affects reliability if just focused on paper work.

### E. Briefing on the NERC Data Request

On Wednesday morning, NERC staff Howard Gugel reviewed with the Team the industry comments and the NERC responses and changes on the draft NERC Data Request *(See Appendix #4)/*
He then presented a summary document showing the results of the six entities whose SDT members responded which included some large and small entities. Although this is a very insignificant sampling as a statistical analysis, it does show a net gain in cyber assets. No one entity showed fewer assets by using the bright line requirement. The SDT will need to categorize by type for the full set in September. The Chair encouraged members to think of questions we could ask of the data that would help our analysis of CIP 002-4.

*Member Comments*

- Looking at high category as equal to "critical." The SDT would be interested in seeing what would be "medium" as a distinction with 010-011 versus CIP-4. This should include high and medium and be a positive number.
- We need to see if we can find the number of "high" – how many more sites would be subject to the standard as a "high?" A: the data from the Data Request should help define that – but does not identify "cyber" assets.
- We will need to document the technical justification for each element of our work
- Responses are in numbers not text to allow for quick compilation in spread sheet form for analysis
- No one listed anything new in category 1.2 – nothing new additional under bright line – none of the six members listed nuclear, though some have nuclear facilities.
- Catch data on switchyards to nuclear? Yes, as the interface which is important to us.
- Generation control centers only exist in "high" or "low" - not "medium" – intended?

# II. SDT CIP 002-4 STRAWMAN DOCUMENT REVIEW

## A. Overview

John Lim provided an overview of the work by a sub-team in refining the CIP 002-4 draft following the Pittsburgh meeting. *(See, Appendix # 6 )* He noted that following its review and refinement at this meeting, the SDT will seek to adopt it to provide a draft to the NERC staff for their review and proposed edits. In Winnipeg the SDT will review and analyze industry responses to the Data Request, review the NERC staff edits to the CIP 002-4 with the VSLs and VRFs, and review and refine several associated documents including: an implementation plan, a guidance document including rationales for Attachment 1 and a summary of industry informal comments on CIP 010 Attachment 2, on which CIP 002-4 Attachment 1 is based.

Phil Huff and Howard Gugel took notes on possible rationales and justification and checked with the SDT periodically following discussions to clarify the justifications. Their notes will be used to develop the justification draft following this meeting.

## B. Review and Refinement of the Strawman CIP 002-4

The SDT reviewed each section of the CIP 002-4 strawman, and as needed, conducted straw polls on the acceptability of the language. The final adopted text is included in Appendix #5 and a full set of SDT comments and polls is included in Appendix #6.

### 1. Applicability

**Distribution Provider**

***Straw Poll*: Support removing distribution provider from the applicability section. Yes-15 No-4 (74%)**

SDT comments included: helps to improve possible industry acceptance in balloting; Version 3 did not have this; wait for CIP 010 and 011 to re-introduce as responsive to Order 706 and could be an attack vector will need protection

**4.2:** SDT question: What was the rationale for taking out this section? It is covered under 706b – no longer exempt.

**4.2.1 - last sentence added**
***Straw Poll*: Favor removing "However all access points to the ESP are not exempt.": Yes-16 No – 0 (100%)**

The SDT discussion before the straw poll included the following points: this comment belongs to the requirements; this clause is already in CIP003; why include one item here but not serial dial up; and, clarifying what is on or off a list, not the protections required.

**2. CIP 002-4 Requirements**

John Lim noted that the SDT agreed in Pittsburgh to delete the original R1. This is modified version of the original R2 in Version 3 which was accepted in Pittsburgh.

**R1.** Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the ~~create, maintain and review on an annual basis, a list of its Critical Assets identified according to the~~ criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

**Re-insert the original R1 language on annual review**
***Straw Poll*:** support using the original language (underlined above):
**Yes - 17 No – 0**

Discussion before the straw poll resulted in some edits to make the statement clearer. Other comments before the straw poll included: whether to leave "annual" as it is here or whether to stick with the original R1 language; should acquisition of new assets be included here; and should this address including new asset as a CA and not waiting until the end of the annual period

**R2.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets. ~~essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real time power system modeling and real time inter utility data exchange.~~ For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

Member comments on R2 included: changes made in R2 need to be consistent with Attachment 1; change "essential to operation" because it may leave too much flexibility

for entities; NERC Glossary definition of CA includes "essential" to operations; worried about how rather than what they are doing; moving it is a way of mitigating the risk; examples and definitions should not be in the requirement; and add a box explaining it is redundant and is covered by definition.

The SDT tested the following changes with straw polls:

***Straw Poll*:** Remove "essential to operation of the Critical Assets":
**Yes - 13 No – 6 (68%)**

***Straw Poll*:** Remove Examples sentence –
**Yes - 15 No – 4 (79%)**

- Opposed. The SDT should take minimalist approach to editing so as to avoid comments on why language is removed. We can address many of these in CIP 010-011.

***Straw Poll*: Put Last sentence above**
**Yes 19 No- 0**

- M1 was removed earlier and needs to be noted in the final redline

### 3. Critical Assets Criteria- Attachment 1

The SDT reviewed, refined and tested the criteria listed in the CIP-002-4 strawman prepared in advance of the Chicago meeting. As a result of the Chicago discussion, straw polling and refinements to the criteria taking place on Tuesday and Wednesday *(See Appendix 6 for the SDT discussion notes and straw polls)*, the following 16 criteria were adopted unanimously by the SDT on Thursday morning for review by NERC staff before the Winnipeg session:

1.1. A generating unit or group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed.

1.2. Any reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3. Generation Facilities that the Planning Coordinator or Transmission Planner designated as required for reliability purposes.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and initial switching requirements identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.
1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with four or more other stations in the Eastern Interconnection or the Western Interconnection.
1.8. Transmission Facilities operated at 200 kV or higher at stations interconnected at 200 kV or higher with four or more other stations in the Texas Interconnection or the Quebec Interconnection.
1.9. Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
1.10. Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
1.11. Transmission Facilities providing the generation interconnection required to directly transmit generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified in Attachment 1, criteria 1.1 or 1.3.
1.12. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
1.13. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
1.14. Common control system(s) that are capable of performing automatic load shedding of 300 MW or more.
1.15. Any control center or control systems, and backup control center or backup control systems, used to perform the functional obligations of the Reliability Coordinator or Balancing Authority or Transmission Operator.
1.16. Any control center, or backup control center, used to control generation that is identified as a Critical Asset, or used to control generation greater than an aggregate of 2300 MWs in a single Interconnection.

**C. CIP 002-4 Implementation Plan**

**1. Initial Proposed Approach**

Scott Mix reviewed the a proposed approach for the Implementation Plan with the SDT which is based on utilizing the currently FERC approved CIP implementation plan and included the following components:

**Proposed Effective Date Language**

- "The first day of the first full calendar quarter after applicable regulatory approvals have been received; or, the first day of the second full calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required."
- *Assuming* FERC acts within one quarter, issuing an order on March 31, 2011, the effective date would be July 1, 2011 in both the US and Canada.
- Outreach to inform industry to start identification process upon filing.

**The Rest of the Standards**

- Since we aren't making changes to CIP-003 through CIP-009, the currently approved "Implementation Plan for newly Identified Critical Cyber Assets and Newly Registered Entities" would apply
- This plan was designed to apply to "Newly registered Entities", and was modeled after the Version 1 Table 4.
- Assuming the previous timeline, the starting date for this plan would be July 1, 2011.

**Newly Identified CCA Plan Recap**

- The Newly Identified CCA Plan allows:
- •24 months for entities without any Version-3 CCAs
- •For entities with Version-3 CCAs:
- Immediate for Policy, Leadership, Exceptions (CIP-003), Awareness (CIP-004)
- 6 months for Information Protection, Access Control, Change Control (CIP-003), Incident Reporting and Response (CIP-008), Recovery Plans, Backup & Restore, Testing Backup Media (CIP-009)
- 12 months for Electronic Security Perimeter (CIP-005), Physical Security (CIP-006), Systems Security Management (CIP-007), Exercises, Change Control (CIP-009)
- 18 months for Training, Personnel Risk Assessment, Access (CIP-004)

This approach was presented in Pittsburgh to the SDT and then refined based on that discussion. He noted the schedule assumes for a FERC order on the last day of a quarter and suggested the proposal is aggressive achievable and probably meets FERC's expectations. He suggested that 24 months would not be acceptable to FERC based on past experience. The Chair suggested that following the review and testing of approaches he would look to forming a drafting team to develop a proposal for review and adoption in Winnipeg. (See Appendix #7 for the full set of discussion notes.

Member and participant discussion comments on the approach touched on: the importance of a communication plan**;** the likelihood of FERC Approval of the plan; the impact of bright lines on timing questions; the ability to budget for these changes; whether the information from the NERC Data Request will help guide the implementation plan draft; the newly identified CCA plan; and nuclear generation.

**2. Revised Approach Concept**

Following the discussion of the approach above a revised concept statement was presented by John Lim and Scott Mix providing:

> "For the initial implementation of CIP 002-4, CCAs at newly identified CAs will be 24 months (i.e., follow Milestone Category 1 in Table 2, Implementation Milestones for Newly Identified Critical Cyber Assets) in the IPFNICCAANRE (Add 706B items and TFEs)
>
> For subsequent implementations of CIP 002-4 at newly identified CAs, the IPFNICCAANRE will be followed as written
>
> For all implementation of newly identified CCAs at existing CAs will follow the IPFNICCAANRE as written."

The discussion of the revised implementation concept included: clarifying its approach as covering the one time exemption/override for 24 months for newly identified CCAs at newly identified CAs but with everything else is consistent with existing effort; factoring in 706b and when to file TFEs; clarifying how this implementation plan would impact or be impacted by the new CIP 005 version; covering the need for outages to implement.

***Straw Poll on Proposal***
**Favoring proposed approach to drafting implementation plan**
**Yes=9 Oppose=4 Abstain=5**

### 3. Alternative Approaches to Developing the Implementation Plan

Following the poll the SDT identified and discussed the following potential alternative approaches:

a. Implementation plan that requires identification of CAs within 1 quarter and CCAs in 4 quarters. Existing Newly Identified CCA Plan could be used (but the clock would not start for these new CCAs until 4 quarters (12 months) after approval

*Or*

b. Develop a new implementation plan that allows
   1. 24 months for Newly Identified CCAs and New CAs and
   2. Uses the existing Newly Identified CCAs for New CCAs at existing CAs
   3. Keep the newly identified CCA

*Or*

c. Add one quarter to Scott Mix's original plan for effective date.

*Or*

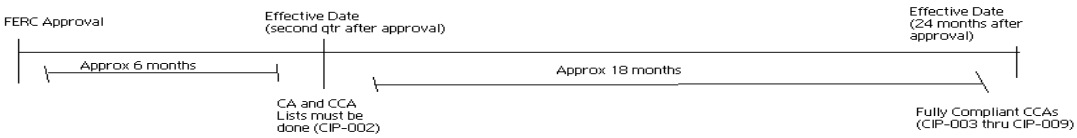
d. Develop a one-shot/one time exception (for specific circumstances) with a sunset to the existing implementation plan schedule.

*Or*
e. Provide six months for identifying and 24 months to comply.

Member discussion of potential alternatives included: clarifying the impact and pros and cons of each option in terms of the possibility of opening up the implementation plan and delaying FERC's approval; the observation that the issues affect mostly generation with some transmission; consider these options from an audit enforcement perspective; the visibility of a clear date is critical to show moving forward on implementation; It will be easier to justify if tied to the a already FERC approved implementation; general agreement on the concept but we haven't settled on the length for compliance. Following this discussion, over lunch John Lim and Scott Mix drafting the following revised concept:

**For the initial application of the "bright lines" in CIP 002-4, CCAs at newly identified CAs will be compliant at 24 months from identification (add 706B items and TFEs)**

**The effective date of the standard (upon the regulatory approval) the registered entity will need to identify CAs and CCAs within six months and xx months to be compliant with 003-009**




## 4. Implementation Plan Drafting Team

The Chair and Vice Chair thought there was enough input for a drafting team to develop a new proposal and solicited volunteers for a drafting team to bring back for the SDT's consideration in September.

**Implementation Plan Drafting Team Volunteers**: Sharon Edwards, Dave Revell, Kevin Sherlin, Scott Rosenberg, Mike Keene (FERC), Dave Norton and Phil Huff and Scott Mix.

# III. REVIEW AND DISCUSSION OF CSO 706 SDT CIP 010 & 011 DRAFT WORK PLAN AND SCHEDULE

## A. Initial Review and Discussion of CIP 010 & 011 Schedule and Workplan

On Tuesday morning, Phil Huff presented a strawman draft 010-011 schedule circulated to the SDT prior to the meeting and asked Allen Mosher to provide the Team with any feedback prior to its fuller discussion and adoption on Thursday. Phil reviewed meeting schedule with approval for posting for 45 day formal comment in late May and with no informal postings between anticipated based on experience and feedback earlier this year with CIP 011 & 012.

Mr. Mosher suggested the SDT may still want to consider an informal comment period. John Lim noted that we have tended to get the same comments for both informal and formal postings and the industry has been confused when the informal draft is incomplete. They might appreciate dealing with as complete a package as possible. He noted the SDT's hope and expectation is that if NERC can develop a good communication plan, it can prevent or minimize the confusion and reduce the anxieties as well as allow for some informal feedback. The Team should be providing what is the standard, along with an explanation of the rationale and build in multiple rounds of formal comment. The draft schedule proposes at least three rounds to build expectation and understanding allowing the SDT to refine and focus on the key issues for industry acceptance.

One company has estimated $150 million to implement CIP 010 and 011 and the chance for companies to provide informal input is vital now that it is mandatory with huge fines potentially. The visibility of this effort is high as is the industry anxiety. For example, one potential unintended consequence may be that companies would shut down marginal plants rather than implement the new cyber security requirements.

Investments in cyber security should be aimed at highest benefit. Some entities are hiring compliance officers to check boxes focusing on the trivial. This is a problem in current CIP 002-009 standards. Cyber security is not vegetative management. Rather it is fundamentally different effort in terms of enforcement. The industry may need a system of certification. There is anger out among entities about compliance with CIP 002-009. We may need to look at the FSMA model for certification methodology and lessons learned.

How do we agree on a schedule if we do not have general acceptance of our approach to CIP 010-011?

## B. 2nd Review and Refinement of Workplan and Schedule for CIP 010-011

On Thursday, the SDT took up the review of the schedule and tasks for completing its work on the CIP 010 & 011. Phil Huff reviewed with the Team the key highlights of the draft schedule:

- First posting for Formal Comment is proposed for May 31, 2011.
- This assumes an aggressive NERC industry communication campaign to support the effort prior to posting for formal comment.
- By December the SDT will turn its full time attention to CIP 010 & 011.
- By March the SDT will send a package for review with NERC staff, compliance and legal.
- Review in April any edits and Approve in May.

There was and extended SDT member and participant discussion that covered many issues (*See Appendix #7 for a detailed version of the comments).* Stu Langton suggested there was an important discussion of three distinct issues: schedule; preliminary work on next phase; and deeper issue of approach to drafting during the next phase. We may need someone to work on and present a suggestion on the drafting approach for the next phase in Winnipeg.

The discussion on Thursday afternoon covered the following topics:

- Schedule & industry confusion and communication
- Clarifying SDT deliverables- short and long term
- Sub-team role in setting out proposed approach for full team SDT review.
- SDT organization and management in 2011
- Clarifying the SDT's overall approach to CIP and validating the work to date
- The role of security and costs in designing the CIP standards approach
- Clarifying FERC's direction to the SDT
- Clarifying the problem the SDT is addressing- including reviewing the SAR
- NERC's investment and expectations of the SDT getting the job done.
- Conflicting industry and regulator expectations
- The need for high level of communication with the industry in 2010 and 2011.

On Friday morning, John Lim reminded team members of importance of working together as a team. He then withdrew his motion on the proposed CIP 010-011 schedule from day before for the sake of inviting another motion that may be clearer and reflect the good discussion points from yesterday.

Phil Huff offered two motions (seconded by Dave Norton) that describe a process for moving forward on foundational concepts discussed yesterday. In general, the motion moves the posting date for formal comments back to July, 2011 and suggests taking time in front end to set foundation before launching into the requirements in January 2011. This will provide for at least three more months for the foundation discussion. In the course of

discussion of the motion, there were several amendments to the language of motion accepted by the maker and the following motion was adopted with 16 members in favor and 1 opposed:

**1st Motion for CSO706 SDT Project Schedule**

> **The CSO706 SDT will prepare a complete package for initial posting to the industry for consideration and ballot in July 2011, in response to FERC Order 706, with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without major redirection of SDT efforts.**

Phil Huff offered his second motion (seconded by Dave Norton) that established a framework sub-team to be chaired by Dave Norton and will report back to the SDT in October for initial input and then in December for review, refinement and adoption of the CIP 010 & 011 approach. The discussion that followed noted that the motion draws on the essence from Phil's initial proposal (*See Appendix 8).* The following motion was adopted unanimously with 17 members in favor and none opposed:

**2nd Motion Process for Implementing CIP 010-011 Schedule- Framework Sub-Team**

> **The CSO706 SDT will form a sub-team to develop a framework for presenting and scoping cyber security requirements for preliminary delivery in October 2010 and completion in December 2010. This would include the form of the standards and the basis by which the requirements are written and applied. The output of this team would go before the full-team for review and approval. This task would not include the actual development of security requirements.**

The Chair asked for volunteers for the Framework Sub-Team and the following members responded: Dave Norton (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford and John Van Boxtel. In addition, Mike Keane and Scott Mix will join and Joe Bucciero will serve as facilitator. It was agreed that Joe Bucciero would send a note to those members of the SDT not present asking for others who might want to volunteer.

Following the vote the SDT agreed on the following direction to the current CIP-011 Sub-Teams: We need the output from the sub-teams on responses to industry comments and workshop comment summaries so they can be posted in October and recognize industry's investment into those comments.

## IV. DISCUSSION OF URGENT ACTION SAR FOR CIP 005

Scott Mix provided an overview of the SAR and process to date. He noted the following link in the Board of Trustees packet that has the SAR information: http://www.nerc.com/docs/standards/sc/sc_081210a_complete_agenda_draft.pdf

He noted the draft Removes R2.4 and a new requirement R6 on remote access controls – attempts to capture what you do with cyber stuff from outside that needs access inside for remote maintenance and support. This an attempt to bring sanity to the issue and discusses process, procedures and who can do what. The 6.3 protocols for access through ESP still need a guidance document to explain the architecture. R6.5 was deleted – list of technical requirements of what you need to do to those remote sites to secure them. Next steps in urgent action will post the SAR and proposed modifications for comment but not sure if informal or for ballot and formal comment.

*Member Comments*

- Have not seen SAR – concern about requirements in CIP 006 that send you back to CIP 005 – would SAR allow us to clarify R2 and R3 to say you do not have to create an ESP, and would anything here create difficulty with physical access control?
- Effort was to narrowly address issue in the SAR, not open it up to broader issues. You would protect like an ESP without necessarily creating an ESP.
- Physical access control spans geography – treat like an ESP but not create one –
- Send me an email of your and others experience in audits and can look at CAN interpretation.
- Huge issue for our budget and WECC auditors have a different interpretation.
- Multiple ways to address the issues in R6 draft – guidance to auditors will be important
- It says what ought to be done, not how to do it – expectation that multiple correct answers to get the results – auditors need to understand there are multiple possible answers and not just the one they would have done themselves
- R 6.5 – original team intent – meant that outside device needed protections – if R 6.5 is out then need support contracts should require support to follow rules.
- How do you audit it if it is not in the standard?
- Put into guidelines at a minimum – also 6.3.1, host inside the end point or something else? Could create problems as written.
- Can't look at encrypted info as it crosses?
- Members should consider providing comments to spur team to look at the issue
- We are making conforming edits – is that included here or vice versa?

- NERC staff proposes references 005 to this posting. NERC will have to conform the two so not to complicate this teams work and avoid auditing confusion
- Any of the language from CAN or our work make it into this version? Do we need to do something in our version to incorporate the CAN? Would the CAN end up defining the requirement?
- This process will potentially create implementation and audit questions – what can we live with from an operational perspective – CAN addresses something we did not get to yet – not sure we have time and ability to fix it now, but may when we go back to 010-011 may need to consider it as input to that later work.
- How does this integrate with 004? Does it creates double jeopardy? CIP 003 lays out the governance, CIP 004 says who can have access, CIP 005 says how they can have access.
- CIP 004 seems to overlap with changes presented here – should we look at cleaning up the potential mess of remote access?
- SDT members should use the process for providing comment to get the new group to look at it – official documentation to ensure they look at it.
- Does the SAR allow them to look at CIP 004 to address?
- When will it be posted? Not sure of the mechanics of the posting, but the NERC BOT has authorized to post and the announcement may be soon, sometime new week.
- Who is working on conforming these two efforts? The industry will not care who it comes from. This should be put on the webinar call in September to educate the industry. It is a very complex topic.
- There will be comments on CANs too.
- Need to keep focus more narrow – and suggest Ed Goth as author of the SAR participate in the webinar and provide a one page summary *(Scott Mix will reach out to Ed)*
- Looking at interactive remote access or any remote access – the controls offered here all seem aimed at interactive remote access – does not say support and maintenance
- File a comment for clarification

## V. NEXT STEPS AND ASSIGNMENTS

The Chair and Vice Chair discussed with the SDT the Winnipeg agenda. The meeting will start Wednesday morning, September 8 through mid-morning Friday, September 11. The meeting will include the final adoption by the SDT for posting of 002-4, a review of the results from the NERC Data Request and their tabulated database results to determine whether any criteria need changes, and review of a CIP 002-4 comment response document drawn from the relevant comments on Attachment 2 of CIP 010 informal posting.

Brian Newell has offered to create a database that the SDT can use to calculate the NERC Data Request question totals. This will be sent around for the SDT to review in advance of Winnepeg.

Herb Schrayshuen, NERC, noted the discussion of whether additional project management service is needed. The Chair suggested that the SDT will develop better clarification of scope for CIP 010 and 011 after December, 2010 discussions of the Framework sub-team and that a review of the need would be performed at that time.

The chair also noted the need to start working on planning for theSDT CIP 002-4 webinar to be conducted on September 23rd from 11:00-1:00 EST. It makes sense that the CIP 002-4 subteam lead the webinar presentation(s) with other SDT members providing technical support and NERC and others to provide industry support. A proposal going forward will be reviewed and adopted the Winnipeg meeting.

The Framework sub-team is planning to meet approximately twice a week on Monday and Thursday afternoons starting the week of August 23 for approximately 90 minutes to accomplish its objectives. Joe Bucciero will be sending out a scheduling tool to select the best meeting times for most people to participate.

Stu Langton noted that last month the SDT talked about setting aside a once a month conference call midway between their meetings which could be cancelled if not needed. The Chair asked Joe Bucciero to send out a recurring invitation to put on everyone's schedule for four hours. The first session will be scheduled for Thursday, August 26, from 12-4 p.m., EDT.

The Chair and Vice Chair thanked Doug Johnson for the excellent hosting and accommodations, especially the Blue Angels demonstration.

*Meeting adjourned at 11:15 a.m.*

## 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)*

**Appendix # 2 Attendees List**
**August 10-13, 2010, Chicago IL**

**Attending in Person — SDT Members and Staff**

| | |
|---|---|
| 1. Rob Antonishen | Ontario Power Generation |
| 2. Jim Brenton | ERCOT |
| 3. Jay S. Cribb | Southern Company Services |
| 4.Joe Doetzl | Kansas City Pwr. & Light Co |
| 5. Sharon Edwards | Duke Energy |
| 6.Gerald S. Freese | America Electric Pwr. |
| 7. Jeff Hoffman | U.S. Bureau of Reclamation, Denver |
| **8. Phillip Huff, Vice Chair** | Arkansas Electric Coop Corporation |
| 9. Doug Johnson | Exelon Corporation – Commonwealth Edison |
| 10. Patricio Leon | Southern California Edison |
| **11. John Lim, Chair** | Consolidated Edison Co. NY |
| 12. David Norton | Entergy |
| 13. David S. Revill | Georgia Transmission Corporation |
| 14. Scott Rosenberger | Luminant Energy (T/W/Th) |
| 15. Kevin Sherlin | Sacramento Municipal Utility District |
| 16. Jonathan Stanford | Bonneville Power Administration |
| 17. Keith Stouffer | National Institute of Standards & Technology |
| 18. John Van Boxtel | WECC |
| *Herb Schrayshuen* | *NERC Vice President and Director of Standards (Th/F)* |
| *Scott Mix* | *NERC* |
| *Howard Gugel* | *NERC* |
| *Joe Bucciero* | *NERC/Bucciero Consulting, LLC* |
| *Robert Jones* | *FSU/FCRC Consensus Center* |
| *Stuart Langton* | *FSU/FCRC Consensus Center* |
| *Hal Beardall* | *FSU/FCRC Consensus Center* |

**SDT Members Attending via ReadyTalk and Phone**

| | |
|---|---|
| 19. John D. Varnell | Technology Director, Tenaska Power Services Co. (T/W) |
| 20.Rich Kinas | Orlando Utilities Commission (T/W) |
| 21. William Gross | (W/Th/F) |
| 22. Tom Stevenson | Constellation (T/Th/) |

**SDT Members Not Participating**

| | |
|---|---|
| Jackie Collett | Manitoba Hydro (W/Th/F) |
| William Winters | Arizona Public Service, Inc. |

**Others Attending in Person**

| | |
|---|---|
| Jan Bargen | FERC |
| Joel Garmen | Next Era Energy (FPL) (T/W/Th) |
| David Batz | EEI (W) |
| Robert Preston Lloyd | Southern California Edison |
| Michael Keane | FERC |
| Jason Marshall | Midwest ISO |
| Bryn Wilson | OG & E |
| Brian Newell | American Electric Power |
| Mark Simon | Encari |
| Tom Alrich | Matrikon |
| Allen Mosher | APPA, Standards Committee Chair |
| Guy Zito | NPCC (T/W) |

**Others Attending via Readytalk and Phone**

**August 10, 2010, Tuesday**

| | | |
|---|---|---|
| Peter | Kuebeck | FERC |
| Todd | Williams | MidAmerican |
| Larry | Camm | Schweitzer Engineering Laboratories, Inc. |
| Michael | Welch | Florida Power and LIght |
| Laura | Hussey | laura_hussey@mindspring.com |
| Thomas | Reina | FERC |
| David | Batz | Edison Electric Institute |
| Andres | Lopez | US Army Corps of Engineers |
| Justin | Kelly | FERC |
| Jerome | Farquharson | Burns & McDonnell |
| Roger | Fradenburgh | Network Security Technology, Inc |
| Rod | Hardiman | Southern Company |
| Nicholas | Snyder | FERC |
| Jacob | Van Wagoner | El Paso Electric |
| Amir | Hammad | Constellation Energy |
| Summer | Esquerre | NextEraEnergy, Florida Power and Light |
| Ingrid | Rayo | Constellation Energy |
| David | Gordon | Mass. Municipal Wholesale Electric Co. |

**August 11, 2010, Wednesday**

| | | |
|---|---|---|
| Jacob | Van Wagoner | El Paso Electric |
| Justin | Kelly | FERC |
| Andres | Lopez | US Army Corps of Engineers |
| Rod | Hardiman | Southern Company |

| | | |
|---|---|---|
| Sharla | Artz | Schweitzer Engineering Laboratories, Inc. |
| David | Gordon | Mass. Municipal Wholesale Electric Co.(MMWEC) |
| Larry | Camm | Schweitzer Engineering Laboratories, Inc. |
| Michael | Welch | Florida Power and Light |
| Maggy | Powell | Constellation Energy |
| thomas | reina | FERC |
| Amir | Hammad | Constellation Energy |
| Jerome | Farquharson | Burns & McDonnell |
| Matt | Dale | FERC |
| Ingrid | Rayo | Constellation Energy |
| Summer | Esquerre | Next Energy, Florida Power and Light |
| Drew | Kittey | FERC |

**August 12, 2010, Thursday**

| | | |
|---|---|---|
| Rod | Hardiman | Southern Company |
| Jacob | Van Wagoner | El Paso Electric |
| Michael | Fischette | Lansing Board of Water and Light |
| Matt | Dale | FERC |
| Thomas | Reina | FERC |
| Jerome | Farquharson | Burns & McDonnell |
| Andres | Lopez | US Army Corps of Engineers |
| Larry | Camm | Schweitzer Engineering Laboratories, Inc. |
| David | Gordon | Mass. Municipal Wholesale Electric Co.(MMWEC) |
| Justin | Kelly | FERC |
| John | Fridye | AT&T |
| Amir | Hammad | Constellation Energy |

**August 13, 2010, Friday**

| | | |
|---|---|---|
| Sharla | Artz | Schweitzer Engineering Laboratories, Inc. |
| Larry | Camm | Schweitzer Engineering Laboratories, Inc. |
| Jerome | Farquharson | Burns & McDonnell |
| Ingrid | Rayo | Constellation Energy |
| Jacob | Van Wagoner | El Paso Electric |
| David | Gordon | Mass. Municipal Wholesale Electric Co.(MMWEC) |
| Rod | Hardiman | Southern Company |
| Matt | Dale | FERC |

## Appendix #3 NERC Antitrust Compliance Guidelines

*See Antitrust Compliance Guidelines read at the beginning of each day's session at:*

*(NEED LINK)*

*The NERC reminder below was read at the beginning of each day's session.*

NERC REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

**For face-to-face meeting, with dial-in capability:**

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

## Appendix #4 NERC CIP 002 Critical Asset Methodology Survey: NERC Responses to Comments Received

**Summary of Comments Received Regarding Proposed CIP-002 Methodology Data Request:**

NERC's proposed CIP-002 Methodology Data Request was posted for industry comment on July 7 for a nineteen-day public comment period. As a result of this public posting, NERC received comments from 65 entities. Summarized below are the overarching issued identified in these comments and NERC's position regarding the issues raised.

***Issue Number 1:*** Nuclear issue

Several entities expressed concern about what appears to be an additional High Impact Rating criterion (1.1. Nuclear Generation Facilities), that has not been present in previous versions of the CIP-002 standard released for comment. Their concern is that this criterion does not seem to be based on any measurable Bulk Electric System impact, but rather on the type of generation fuel utilized, and that this criteria is not an effective method of reliably determining impact to the BES.

*NERC response:* The main purpose of the Data Request is to obtain information that the CIP Standard Drafting Team can use to determine what assets should be included in the bright line criteria for a proposed CIP-002-4. The Data Request is not proposing to define new criteria. It is merely collecting data so that new criteria can be defined at a later point by the standard drafting team to include in a proposed CIP-002 Version 4 standard.

***Issue Number 2:*** Over counting assets

Several entities were concerned about how to count facilities that may meet multiple criteria. It was expressed that additional instructions for the survey would help to avoid potential erroneous "double counting" of assets that meet certain criteria. For example, facilities that have multiple owners should only be counted once. Facilities that serve multiple entities and/or serve an entity operating in multiple regions should only be counted once. In addition, there was a question about whether the Data Request should be filled out for each NERC Compliance Registry entry, or on an enterprise-wide basis.

*NERC response:* In response to these comments, the instructions were modified to clarify that each facility should only be counted one time in the survey responses. Furthermore, owners of jointly-owned facilities should coordinate their response so that those facilities are only counted once. The instructions were also modified to stipulate that the Data Request should be

responded to on an enterprise-wide basis, to ensure that internal facilities were also only counted once.

***Issue Number 3:*** Estimate on Burden Imposed to Collect Data

Many entities stated that the time estimate to respond to the Data Request was not high enough. Almost all comments stated that the estimate to respond would take anywhere from 25 to 100 hours to complete.

*NERC Response:* The estimated time to complete the Data Request was modified to "less than 100 hours" total per entity.

***Issue Number 4:*** Canadian entity issue

One entity noted that this data request is being proposed in accordance with Section 1600 of the NERC Rules of Procedure. This entity stated that "This section clearly states that, within the United States, NERC and regional entities may request data or information that is necessary to meet their obligations under Federal Power Act. This section does not apply to Canadian based entities and we suggest that in the future this is explicitly stated in the text to avoid confusion on the part of Canadian entities."

*NERC Response:* All NERC registered entities, including Canadian entities, are required to comply with the NERC Rules of Procedure. Section 100 of the NERC Rules provide:

> NERC and NERC members shall comply with these rules of procedure. Each regional entity shall comply with these rules of procedure as applicable to functions delegated to the regional entity by NERC or as required by an appropriate governmental authority or as otherwise provided. Each bulk power system owner, operator, and user shall comply with all rules of procedure of NERC that are made applicable to such entities by approval pursuant to applicable legislation or regulation, or pursuant to agreement.

Therefore, pursuant to applicable legislation, regulation, or agreement among NERC and Canadian provincial authorities, Canadian entities are required to comply with Section 1600 of the NERC Rules of Procedure, including responding to this Data Request upon it becoming mandatory by NERC Board of Trustees approval.

***Issue Number 5:*** High vs. Medium

Several entities expressed concern that high and medium impact levels are included on the Data Request. The concern is that both high and medium impact Critical Assets would be used for CIP-002-4, and all of CIP-003 to CIP-009 would apply to both.

*NERC Response:* The reason that both high and medium impact levels are included in the Data Request is to assist the Standard Drafting Team in determining whether the bright line between high and medium is set at the correct level. The team intends to use only the high impact level for a bright line for determining Critical Assets that will then be used to determine Critical Cyber Assets. There is no intent to include a medium level in the proposed CIP-002-4.

***Issue Number 6:*** Data use

Several entities questioned whether the following statement could be stated with certainty:

*This data will not be used as a basis for determining compliance with the currently enforceable CIP-002 through CIP-009 reliability standards.*

*NERC Response:* As noted in the Data request, the information being collected is only to be used prospectively by the drafting team to evaluate a proposed methodology to be used in a future version of the CIP-002 standard. Therefore, the data being collected will not be used as a basis for determining compliance with the currently enforceable CIP body of standards.

**Changes Made to the Survey in Response to Comments and Standard Drafting Team input:**

As a result of comments received and additional standard drafting team ("SDT") review, NERC made the following changes to the survey:

- Changed the references to "drafting team data request" to "NERC data request."
- Modified the reference to "Regional Reliability Organization" to "Regional Entity" based on the list of Responsible Entities in CIP-002-2.
- Changes the estimated number of hours to complete the data request from "less than 24" to "less than 100" based on comments received on the Data Request.
- Clarified that NERC registered entities should respond to the data request on an enterprise-wide basis, and that entities with jointly-owned facilities coordinate their responses for such facilities.
- An explanation of the requirements under the current CIP-002-2 standard was added to clarify the information requested in questions 1 and 2.
- A clarification was made to ensure that each element on the list should be counted only one time.
- A clarification was made that each Critical Asset should be counted only once.
- A modification was made that all NERC Compliance Registry (NCR) numbers for the enterprise-wide survey response be included.

- Question 1 and 2 were clarified to state that the responses should be based on each entity's existing Critical Asset list under the currently-effective CIP-002-2 standard.
- The third column heading was changed for the tables in question 2 and question 3 for consistency.
- Question 4 was added to require entities to report all NCR numbers for their enterprise-wide response.
- Attachment 1 Item 1.1 – "Generation" was changed to "generation" to reflect the fact that generation is not a NERC glossary term.
- Attachment 1 Item 1.2 – changed based on input from the Standard Drafting Team (STD).
- Attachment 1 Item 1.3 – changed based on industry comments and input from the SDT.
- Attachment 1 Item 1.4 – changed to add clarity based on industry comments and input from the SDT.
- Attachment 1 Item 1.5 – changed to add clarity based on industry comments and input from the SDT.
- Attachment 1 Item 1.7 – split into two items to add clarity based on input from the SDT.
- Attachment 1 Item 1.9 – changed to add clarity based on industry comments and input from the SDT.
- Attachment 1 Item 1.10 – split into two items to separate FACTS devices from other devices that prevent IROLs based on input from the SDT.
- Attachment 1 Item 1.12 – changed to simplify wording and add clarity based on input from the SDT.
- Attachment 1 Item 1.15 – changed to limit scope to control systems for load shedding based on industry comments and input from the SDT.
- Attachment 1 Item 1.16 – modified to add clarity based on input from the SDT.
- Attachment 1 Item 1.17 – modified to provide MW levels in order to provide the SDT with data to determine bright line levels, if applicable.
- Attachment 1 Item 1.18 – modified to provide kV levels in order to provide the SDT with data to determine bright line levels, if applicable.
- Attachment 1 Item 1.19 – changed to add clarity based on input from the SDT.
- Attachment 1 Item 1.20 – added to allow entities to include additional assets as Critical Assets based on input from the SDT.
- Attachment 1 Item 2.1 – modified to provide consistency with Item 1.2.
- Attachment 1 Item 2.2 – modified to provide consistency with Item 1.3.
- Attachment 1 Item 2.3 – deleted based on modifications to Item 1.4.
- Attachment 1 Item 2.3 (new) – modified to provide consistency with Item 1.7.

- Attachment 1 Item 2.4 – modified to provide consistency with Item 1.8.
- Attachment 1 Item 2.6 – changed to add clarity based on input from the SDT.
- Attachment 1 Item 2.7 – changed to add clarity based on input from the SDT.
- Attachment 1 Item 2.8 – changed to add clarity based on input from the SDT.
- Attachment 1 Low Impact Rating – changed “Critical Assets” to “BES Elements” based on industry comments in order to add clarity.

## Appendix # 5- CIP 002-4 Adopted Draft (8-12-10)

### Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification
2. **Number:** CIP-002-4
3. **Purpose:** NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

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

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

   Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.
4. **Applicability:**
   - **4.1.** Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:
     - **4.1.1** Reliability Coordinator.
     - **4.1.2** Balancing Authority.
     - **4.1.3** Interchange Authority.
     - **4.1.4** Transmission Service Provider.
     - **4.1.5** Transmission Owner.
     - **4.1.6** Transmission Operator.
     - **4.1.7** Generator Owner.
     - **4.1.8** Generator Operator.
     - **4.1.9** Load Serving Entity.
     - **4.1.10** NERC.
     - **4.1.11** Regional Entity.
   - **4.2.** The following are exempt from Standard CIP-002-4:
     - **4.2.1** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the

Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

## Requirements

**R1.** Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

**R2**. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

**R 2.1** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
**R 2.2** The Cyber Asset uses a routable protocol within a control center; or,
**R 2.3** The Cyber Asset is dial-up accessible.

**R3.** Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

## Measures

**M1.** The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

**M2.** The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

**M3.** The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3.

## Compliance

**1. Compliance Monitoring Process**

**1.1. Compliance Enforcement Authority**

**1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

**1.1.2** ERO for Regional Entity.

**1.1.3** Third-party monitor without vested interest in the outcome for NERC.

**1.2. Compliance Monitoring Period and Reset Time Frame**

Not applicable.

**1.3. Compliance Monitoring and Enforcement Processes**

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting
Complaints

**1.4. Data Retention**

**1.4.1** The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.5. Additional Compliance Information**

**1.5.1** None.

**2. Violation Severity Levels (To be developed later.)**

## Regional Variances

None identified.

VERSION HISTORY

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | January 16, 2006 | R3.2 — Change "Control Center" to "control center" | 03/24/06 |
| 2 | | Modifications to clarify the requirements and to bring the compliance elements into | |

| | | | |
|---|---|---|---|
| | | conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | | Updated version number from -2 to -3 | |
| 3 | 12/16/09 | Approved by the NERC Board of Trustees | Update |
| 4 | 09/?/2010 | Modified to provide bright-line criteria for the identification of Critical Assets. | |

## CIP-002-4 - Attachment I

### CRITICAL ASSET CRITERIA

The following are considered Critical Assets:

1.1 A generating unit or group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed.

1.2 Any reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3 Generation Facilities that the Planning Coordinator or Transmission Planner designated as required for reliability purposes.

1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5 The Facilities comprising the Cranking Paths and initial switching requirements identified in the Transmission Operator's restoration plan.

1.6 Transmission Facilities operated at 500 kV or higher.

1.7 Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with four or more other stations in the Eastern Interconnection or the Western Interconnection.

1.8 Transmission Facilities operated at 200 kV or higher at stations interconnected at 200 kV or higher with four or more other stations in the Texas Interconnection or the Quebec Interconnection.

1.9 Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.10 Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.11 Transmission Facilities providing the generation interconnection required to directly transmit generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified in Attachment 1, criteria 1.1 or 1.3.

1.12 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.13 Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.14 Common control system(s) that are capable of performing automatic load shedding of 300 MW or more.

1.15 Any control center or control systems, and backup control center or backup control systems, used to perform the functional obligations of the Reliability Coordinator or Balancing Authority or Transmission Operator.

1.16 Any control center, or backup control center, used to control generation that is identified as a Critical Asset, or used to control generation greater than an aggregate of 2300 MWs in a single Interconnection.

## Appendix # 6- CIP 002-4 8-10-12, 2010 Discussion Notes and Straw Polls

In Pittsburgh the SDT, after consideration and debate, agreed to delete Criteria 1 related to nuclear industry generation facilities. The SDT in Chicago looked once again at the possible justifications for restoring this deleted criteria and including nuclear generation facilities. Some argued that if one nuclear plant were subject to an attack then all plants might be shut down until they can prove that they do not have the same reliability issue. This would be a fleet issue unique to nuclear generation and reaction to one incident. In addition once a nuclear plant comes off line it will not get it back in 24 hours – investigation will take time and may take out a big block of production. It is also a symbolic target beyond other system assets that plays in Congress or the New York Times and risk protection strategies need to recognize a higher level of scrutiny and perception.

*SDT Member and Participant Comments*

- **Nuclear facilities.** Agree if higher "value" target then should have more protection, but not because of loss of capacity. No question these plants have high political visibility. However, U.S. has a better, more diverse system of nuclear operation systems. Problems encountered in the past have not shut down all plants.
- We also have the survey to identify which components in nuclear are safety and subject to NRC and which are reliability for NERC – some argue designating all as safety for NRC regulation – may want to designate it all as "high" to avoid issues with NERC.
- NRC has a huge program around cyber security and we are not addressing their issues in the CIP as we are focused on reliability
- Still a fuel question
- Support including – it is optics – high impact, very low probability – but must have standard to address it – exception to calling out a fuel type because of optics
- Communication team needs to explain it was not exempted before but included here – what difference if it is on CA list make any difference in NRC shutting them all down – take exemption out will not affect NRC shutting them down or not for safety
- Would NRC close them all down? Even if they did would do it so as not to affect system reliability – the cyber equipment varies between the nuclear plants, not a common load failure question – this is not a reliability question, only an optics or political question
- We are addressing "impact based" criteria in CIP 002-4 – Hard to reconcile the risk basis for a higher profile for nuclear generation where everything else is impact based, not risk based. This represents a different framework for criteria.
- Political reality – the communication efforts need to point out that we took out the exception for nuclear – if there is a reliability basis, that should be in there – not because it is a nuclear plant.
- Shouldn't matter what the fuel but rather what is the impact on the system. There is a lot of work going on to address the issue within the nuclear industry already.

- Nuclear excluded in Pittsburgh but if exclude 1.1 then may need to add back in – optics must be considered – not mentioning nuclear anywhere will look bad.
- Cyber requirements being developed for nuclear as part of its licensing structure – even though aimed at radiation releases, it is broad and in depth covering the same components for reliability.
- To be consistent it has to be reliability based – but optics that "nuclear" is different or special to those outside the industry.
- How can we focus on reliability of BES but somehow recognize "nuclear"?
- Agree on objectives but how do we get there and arm representatives in Washington – again, in 010-011 some nuclear plants may fall into "low" category – that will not sell – if not including all nuclear then need to explain that NRC is covering under "safety" or other reason – also still believe fleet of nuclear is different and subject to broader potential shut down.
- We will need a clear explanation why any are not included as "critical"
- If use bright line – then many nuclear units will not be included and it will be difficult to defend.
- If put in all nuclear plants now then put in tiered approach later, we may cause confusion – prefer removing exemption and consider the same as others.
- Transmission owner controls substations – most of the nuclear substations are critical even if the generator is not.
- Think we can still say in the next round that all nuclear are "critical"?
- All nuclear generation is addressed by NRC and we say all controls are "high" in our system.
- 1.12 has language already addressing the issue. Nuclear exclusion not there, transmission facilities covered in 1.12 and no distinction by fuel.
- Clarify the shared component is cyber and not just a fence –
- 706b speaks to the issue – anything not covered by NRC is subject to the NERC standards – order by FERC sets out the division of responsibility – no need here to call out the fuel.
- Does not answer if nuclear plant is a CA or a CCA which is necessary to determine 002-009 coverage.
- Either identifying everything inside a common fence, or the common cyber connections
- May help with optics – but the point is to get a list of CCAs – isn't the end result the same – is this plant critical – yes, if it has shared critical cyber asset.
- Have to justify the bright lines you pick to the Commission.
- Trying to in a single section work through an "if, then" set of logic? Single asset for common failure threat or by cyber connection? Just trying to get into the first bucket of identifying as CAs then determine the process for protecting – you seem to be wrestling with both at the same time with the same criteria.
- Will need to show why or how the bright line approach provides better protection
- Any of the alternative language will be "fudgy" and imperfect

- The language in the yellow should be “generation plants” instead of “generation units”?
- Prefer keeping language the same or close to the current CIP version 3
- “For each group of generating units (including nuclear generation) at single plant location identified in Attachment 1 ….”
- Are we saying “only” Cyber Assets that must be considered …? Only shared assets?
- Still needs to be connected by routable protocols – also FERC referred to not enough assets identified, is there a study for that?
- Want to limit the scope to cyber system that controls more than one unit – need to recognize many systems may be interconnected, beyond just the control systems
- In CIP 10 we refocus on cyber systems that impact bright line in 1.1 – here, the clarification smoothes that transition – if we bring everything else in the plant that changes the dynamic – leave this here as is.
- Is there is a concrete definition of adverse impact within 15 minutes – fuzzy, may need discussion later
- Units may talk to each other over some connection – are we considering that a shared system and the only thing we are protecting – what if it is an Ethernet cable without other connections? If it has a switch? What are we trying to get at here? Do we want to protect a cable inside a plant? Are we only looking at “shared”? Does that mean we are protecting cables and switches?
- Tied more to shared systems – it is a connectivity question.
- Shared switch in the middle currently has to be within a protected perimeter.
- Plants surrounded by a fence to be critical only if shared system that impacts the whole site – fence does not define as a critical asset.
- That is not what the standards says – identify those critical to operation of the plant.
- Today protecting assets critical to the unit, not the plant – only those that are shared.
- Can have one cyber asset affecting one unit that then impacts other units – it is the impact on the aggregate of the plant – looking for cyber assets that link the physical assets together – that is what CIP 10 intends to do, but CIP 002-4 does not – find critical assets first through aggregate that exceeds bright line, then for the shared systems.
- Shared systems, not the physical fence
- We should not rely just on the compliance document.
- We had this discussion under “target of production” thirteen months ago
- We should keep the language here or take it out altogether.
- Why does highlighted language not address the issue.
- Switch on the shared network? What needs to be protected? Just the switch?
- Similar problem with EMS – call our control systems as critical.
- How is industry digesting the ambiguity?
- 010-011 addresses the issue, the CIP 002-4 does not.

- The single location is the problem here – I have separated systems and protections even where they are in the same physical location – now trying to introduce a single plant location.
- Delete everything in color – figure out the iron impacted and protect the routable protocols – cannot write something to every entity in the country.
- But we set bright lines and will be held to audits.
- Frustrated because we are trying to define critical asset list when we should focus on the critical cyber asset – this language makes the audits so much more painful.
- Where should we identify the critical asset impact – not critical because it is in the fence but because it impacts reliability.

***Straw Poll*:** Putting in Nuclear as Separate Criteria
**Yes – 3 No – 13**

- 706b already addresses the issue

***Straw Poll*:** Keep the yellow shaded language in R1remain? (For each group of ...)
Yes – 8 No – 9

*Comments after Poll*

- Note we did not say we did not want the language but do not want it here.
- Ramification of putting language in the attachment?
- Putting into attachment loop CAs into determination of CCAs
- If in attachment then the plant is not identified as CA lowering the number identified

**Criteria 1.1 (newly numbered)**

- Wording in 1.1(a) revised to delete 1.1b – (b) was the value if not in a group –
- Value in b sets at smallest value of (a) fluctuating value as a floor.
- (a) was suppose to be RSG and b is if BA is independent – were separated originally
- Thought we said everyone has to be in a group in "a" and eliminated a, b and c
- Can this be accurately explained in a quick manner? Looks as if plants would fluctuate in and out of qualifying
- Is it the lesser of or the greater of? Need to clarify.
- Contingency reserve set differently by region – with guidance from another standard
- Has to be based on a formula
- Standards says there will be a contingency reserve but not prescribe how
- delete "a" and "b"?
- contingency reserve means something to operators – the 2000 is a default number
- Options: delete b, or take 2000 out

- Do we need to put qualifying language back into "a" that was pulled out to make "b"?
- Trying to limit the tracking of different values
- Update as necessary?

***Straw Poll*:** Delete "b", with a and c remaining.
**Yes – 15 No– 0**

- How do we set how determine the value if it fluctuates?
- Reword "a" – "The lowest contingency reserve identified by the reserve sharing group or balancing authority if it is not a member of a Reserve Sharing Group, at the time the CIP002 is reviewed , or….."
- Why set at lowest level? That is the worst case.
- Those are the periods when most vulnerable as units are most likely down for maintenance.
- The lower the contingency reserve the more units are brought in – the contingency reserve is intended to protect your system.
- What is the current level? About 1800, with lowest around 1400-1500

***Straw Poll*:** Support reworded "a":
**Yes – 17 No – 0**

- Some areas that do not have contingency reserves? If required why have "c"

***Straw Poll*: Delete "c"?**
Yes - 10 No - 0 Abstain - 6

- Abstainers need to be educated to know how to vote.
- This was intended to catch any entity that was not in a BA or a RSG
- Everyone has to be in a reserve sharing group.
- A plant can be divided up into four regions – but if so, then it may not be critical – do you need a critical value
- Do we still need to keep the 2000 threshold?

**1.2**

- What group of Facilities within 15 minutes? Need to fix.
- Seems inconsistent with the previous section – this says reactive resource – put comma between compensator and that so we get intent of not associated with Generation Facilities - "any reactive resource not associated with Generation Facilities ….
- If control center controls distribution of cap banks? Combination of all of them could exceed 1000 –
- It makes individual cap banks a CA

- Excluding control centers? It is not a common cyber asset; not sure this sentence says that – change group of facilities to operation of the reactive resources
- Why did we add the "shares a common Cyber Asset or common Cyber Assets"?
- Put period after Cyber Asset and start new sentence?
- Talking about Cyber Assets? Figure out CCAs later
- Any reactive resource at a single location? Excluding generation facilities?
- Any reactive resource or group of reactive resources at a single location (excluding generation Facilities) having aggregated rated net Reactive Power capability of greater or equal to 1000 MVAR
- If no routable protocol or dial up then don't need to worry about shared
- "Nameplate rating"? put back in place of greater or equal to
- Any reactive resource or group of reactive resources at a single location (excluding generation Facilities) having aggregated net Reactive Power name plate rating of 1000 MVARs or greater.
- Take out first "rated"
- Where did we get the 1000 MVARs? Arbitrarily half of 2000 formerly in R1?

1.2 Any reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

***Straw Poll*:** Accept 1.2 as revised above.
**Yes – 16 No – 0**

**1.3**

- "Must run"? It has a specific meaning in certain markets. Planning coordinator doesn't determine reliability "must-run" – not sure who still uses the term. Is there a standard for "must-run"? It is a market thing in our area. There are references on NERC site for "must-run" contracts but it is not an official term.
- If planning coordinator says needed for reliability – may need to change the term – "Generation Facilities that the Planning Coordinator identifies as required to be available for reliability purposes."
- "to be available"? "identify as required for reliability purposes."
- Is the planning coordinator the right entity? (yes)
- Planning coordinator can tell you it is a critical asset?
- Think about possible blow-back if saying cannot retire units for purposes of reliability – if cheaper to retire than pay mortgage but now saying cannot take off line?
- Do we run into challenges of PC determining short term operations by requiring continuing for reliability.
- Every bit critical before you decide to retire the unit than after you decide to retire it – why is it not critical before deciding to retire it?

- Not restricting beyond reliability requirement – what if WEC is the designator and the auditor? Is the RRO designating and auditing Critical Assets?
- What is added here not captured in 1.1.
- WEC does have designated "must-runs"
- How do I know what has been identified under this provision? By contract? Then formally designated.
- May not be just a retirement issue.
- Change to "designated" and drop formally?
- What is the time frame? Past, future or current?
- Think it is current when you are audited – that is the way written now.
- Concerned about WEC designating and auditing – seems a conflict of interest, but willing to let industry ballot and comment.
- Add Transmission Planner?
- Care less about who and more about how designated.
- Identified assets we think is critical – let industry decide who and how designated – put out to ballot as written here

"Generation Facilities that the Planning Coordinator or Transmission Planner designated as required to be available for reliability purposes."
Support for 1.3 as revised above:

***Straw Poll:*** Yes: 13 No: 1 Abstaining: 1

1.3

- Transmission operators plan identifies all Blackstart capable units – is that what we intended, to bring in every Blackstart capable unit?
- Need to see what the requirements are for TO to come up with the plan.
- Blackstart is a NERC defined term that may limit – though Blackstart plan includes other resources not included in the term "Blackstart Resources"
- These are not necessarily units you go to first – may need to reach out to drafters of standard to identify the critical assets and not the small units that may be listed in the plans
- "Essential to system restoration" – not everything, but what you would go to first to restore the system – the starting points – restoration plans include anything capable – This needs clarification
- Read NERC definition of Blackstart Unit as background.
- Requirement to test to see if units capable of performing Blackstart function – scheduled test.
- Blackstart units listed to kick in big units – seems clear.
- Large number of permutations for bringing supply back on line? Plan is set out to assure enough capacity is available – blackstart units are declared in current plans.

- Why was "primary" dropped from 1.4? Because there is not distinction or requirement for a "primary" blackstart unit or resource.
- Are we providing incentive to remove assets as blackstart units?

**1.4-1.6**

- How would Blackstart unit know it is included – need to clarify
- The plan is a catalogue of everything capable of serving as a Blackstart Resource
- Definition of Blackstart Resource is not every capable unit
- There are actual contracts out there for Blackstart Resources and contingencies – we have are resources designated.
- How about "contained" versus "identified"?

1.3 Any Blackstart Resource contained in the Transmission Operator's restoration plan.
1.4 The Facilities comprising Cranking Paths contained in the Transmission Operator's restoration plan.

- Phil Huff will check with Rich Kinas this evening who drafted this section at the last meeting.
- Can we say any Blackstart Resource in the plan is in?
- We had "primary" still in the survey? Significant difference between any and primary – may preliminary survey responses may be all wrong
- Can compile and provide quick overview along with some of the initial industry comment in response to the language in the survey

On Thursday morning, the SDT review any final outstanding issues before seeking to adopt CIP 002-4 for NERC staff review.

- **Criteria 1.1**. Regarding yesterday's question about voltage differences between regions – Scott Mix thought there was a reference possible to an existing standard. After some research it does not seem to be any accepted standard we can rely on for justification for differences by region.
- The idea is to identify where the bulk of BES occurs and hope that if you draw bright lines you will capture the highest impact facilities so the cyber assets connected to them will be protected.
- If bright line is from Vegetation, then it is 200 across regions.
- Trying to provide a clear understanding to a complex situation is something like fitting a square peg into a round hole.
- The 200 level gets both worlds with one standard.
- Losing sight of the fact we need three lines for h-m-l – but not a distinction between regions – lowering to the lesser one may not address need for three later on – ultimately will need more than one bright line.

- This does give us room to pick a medium later.
- Do we need three bright lines? This may be a misapplication of the NIST model. Could we get around this if we do high and everything else? Have been vigorous and gone fairly deep with high here, down into the mediums. Some think high should be much higher than here, more included here than many had expected.
- Suggest sticking with what we have at this point – need additional expertise in the room to help determine the appropriate level.
- Still have capability to tier even if we go with 200 cutoff here.
- Distinctions between interconnection on megawatts but different for voltage levels of transmission
- Went with the number based on Texas using 230 – need to confirm what Texas and Quebec use. Most of Quebec is over 300
- Looking at voltage class – may need to look at capabilities
- Allen Mosher suggested looking at getting subject matter experts from other teams to review our product to make sure it makes sense and help with the justifications
- Want a simple to understand bright line solution or appropriate solution to a complex issue – bright lines do not always fit cleanly or provide perfect solutions
- Do not have enough operational expertise on this group – we got review from others in the past – need to do so again – still think we need to draw clean lines the best we can – comment period will allow experts to weigh in on the line
- Anecdotal evidence says we do not need 1.8 – ask Rod Hardiman for advice
- Justification for separate voltage thresholds for Texas and Quebec? Strike criteria if not, and go with one standard. Quebec has said they want 500.
- Justification for distinction between 1.7 and 1.8? Pointing back to a document that cannot be found. I am nervous to make that distinction without more knowledge. From the southeast perspective I am comfortable for deleting 1.8.There is no justification for the distinction
- Threshold may be important – 300 may be justified

***Straw Poll:*** Test whether to strike 1.8, and Eastern-Western from 1.7?
**Favor=15 Oppose=0 Abstain=3**

**Motion to forward CIP 002-4 with attachment 1 to NERC for staff review**
*(Huff, Norton 2nd)*
**Yes=18 No=0**

## Appendix #7 CIP 002-4 Implementation Plan Discussion Notes

Scott Mix reviewed the a proposed approach for the Implementation Plan with the SDT which is based on utilizing the currently FERC approved CIP implementation plan and included the following components:

**Proposed Effective Date Language**

- "The first day of the first full calendar quarter after applicable regulatory approvals have been received; or, the first day of the second full calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required."
- *Assuming* FERC acts within one quarter, issuing an order on March 31, 2011, the effective date would be July 1, 2011 in both the US and Canada.
- Outreach to inform industry to start identification process upon filing.

**The Rest of the Standards**

- Since we aren't making changes to CIP-003 through CIP-009, the currently approved "Implementation Plan for newly Identified Critical Cyber Assets and Newly Registered Entities" would apply
- This plan was designed to apply to "Newly registered Entities", and was modeled after the Version 1 Table 4.
- Assuming the previous timeline, the starting date for this plan would be July 1, 2011.

**Newly Identified CCA Plan Recap**

- The Newly Identified CCA Plan allows:
- •24 months for entities without any Version-3 CCAs
- •For entities with Version-3 CCAs:
- Immediate for Policy, Leadership, Exceptions (CIP-003), Awareness (CIP-004)
- 6 months for Information Protection, Access Control, Change Control (CIP-003), Incident Reporting and Response (CIP-008), Recovery Plans, Backup & Restore, Testing Backup Media (CIP-009)
- 12 months for Electronic Security Perimeter (CIP-005), Physical Security (CIP-006), Systems Security Management (CIP-007), Exercises, Change Control (CIP-009)
- 18 months for Training, Personnel Risk Assessment, Access (CIP-004)

Scott Mix reviewed the above proposed approach for the Implementation Plan with the SDT which is based on utilizing the currently FERC approved CIP implementation plan. This approach was presented in Pittsburgh to the SDT and then refined based on that discussion. He noted the schedule assumes for a FERC order on the last day of a quarter and suggested the proposal is aggressive achievable and probably meets FERC's expectations. He suggested that 24 months would not be acceptable to FERC based on past experience.

The Chair suggested that following the review and testing of approaches he would look to forming a drafting team to develop a proposal for review and adoption in Winnepeg.

*Member and Participant Discussion Comments on the Proposed Approach*

- **Communication plan.** Is there a communication plan for this? Communication is very important

- **FERC Approval**
- Also concerned about FERC approving but asking for changes. Multiple industry avenues to get the information out should be part of the communication plan.
- The SDT is asking FERC to recognize the potential difficulty for implementation if there is an approval that also requests changes. If the industry doesn't know until March 31, then there may be only 3 months to analyze and identify critical assets.
- Can FERC staff take this concept back and ask if this approach is reasonable – can FERC approve in the first quarter of 2011 in order to implement by July 1, 2011.
- FERC staff agreed to discuss and see what other staff (not the Commission) thinks. Still need to address justifications for bright lines, that is the focus of FERC review.
- FERC staff appreciates reliance on already vetted plan – changing effective date to second and third quarter gets us to the current proposal of two full quarters.
- FERC staff suggested that adjusting quarters is a good idea – careful not to open a new can of worms and push approval back past 3-31-1l. Recognize the importance of budget cycles but those are plans, you already have to have every one of the processes listed, just adding items to the process
- This is just for CIP-002 which is only one change. Date could be different than CIP 003-009. Could it be different for CAs and CCAs?
- Can we stagger the implementation of CAs and CCAs? We will significantly increase the number identified and if an entity misses one will they have to self report on July 1?
- Could adjust to second and third full quarters – lock in the end date with interim steps?
- The NERC Board of Trustee approval starts the clock – if FERC request changes, then pushes this back at least 6 months. The pre-work by industry should not be affected. It should be a six-month effort with a nod half way through that the July date is still good.

- **Impact of Bright Lines on Timing.** In terms of the methodology for identifying new assets, we did not anticipate the level of new assets. If an entity identifies a new asset, you have to put new security in place and that will take longer than six months.
- The proposed plan addresses assets that become critical under the new methodology.

- If we propose 24 months for newly identified CAs, this will invalidate the current FERC approved CIP implementation plan.
- In essence, the proposal is the industry gets one year, six months for the approval and six months to implement.
- This may involve implementing a whole new program, not just extending existing program and may be very difficult for the industry to implement.
- As a result of the proposed bright lines, the Industry may have a large increase of CAs and then CCAs. We may need more time for addressing that impact.
- The effective date of any other standard is when you can demonstrate you are in compliance which would be a signed list of CAs and CCAs.
- The six months accounts not just for equipment but also personnel

- **Budgeting for Changes.** Under the existing risk-based approach, you can plan and budget for when an asset comes on or off list. Assuming CIP 002-4 is adopted and approved, you may have to be compliant before you can go through a single budget
  cycle. We should consider allowing for more time in order to budget for compliance.
- We have a fiscal policy but not an unchanging budget. Optically, I believe we cannot push out more than two quarters.
- Understand concern about the budgets, but it sounds like we are afraid because we don't know yet what the impact will be and hopefully will know more once survey results come in, we will have a clearer idea of the impacts.
- Our company is partially regulated in Canada. In the past that we have to wait for approved standards before we can include them in the budget. 12-months may be too dicey

- **Survey Information.** To what extent will completion of survey give industry a heads up? It will tell you something is happening but not what to budget for. The survey does not imply money and there is not implementation plan to reference in completing the survey
- Entities cannot budget based on survey results. The bright lines will require upgrades that may require an outage cycle along with budgeting. Compliance within the timeframe proposed may be very difficult.
- The proposal says time starts once the CA is identified which is July 1, 2011. Having a single date simplifies audits.

- **Newly Identified CCA Plan.** Can we put in the existing implementation in modifications for CCAs? Raises the question of whether we use the newly identified CCA plan or not – if not, then have to redo with new dates.

- **Nuclear Generation.** How do we factor in the nuclear industry? If we address implementation for them, we could leverage that to include new sites.

- If unplugging is detrimental to reliability, we do not want to create reverse incentive to undermine reliability.
- Unplugging may work in some cases but we estimate that we are adding up to twenty plants and possibly $150 million for our company under this proposal. The budget cycle then implementation cycle follows including outages. Unscheduled outages are disruptive, and scheduled outages take time. This is primarily a generation issue with some transmission impacts.
- Consider language similar to the nuclear plans, "no later than X date."
- Need to look at exceptions – what new TFEs need to be in place or filed
- The SDT assign a team to draft new implementation plan and address timing in light of these comments?

**1. Implementation Plan Proposed Concept- Revised**

Following the discussion above the a revised concept statement was presented by John Lim and Scott Mix:

**For the initial implementation of CIP 002-4, CCAs at newly identified CAs will be 24 months (i.e., follow Milestone Category 1 in Table 2, Implementation Milestones for Newly Identified Critical Cyber Assets) in the IPFNICCAANRE (Add 706B items and TFEs)**

**For subsequent implementations of CIP 002-4 at newly identified CAs, the IPFNICCAANRE will be followed as written**

**For all implementation of newly identified CCAs at existing CAs will follow the IPFNICCAANRE as written.**

*Discussion of Revised Concept:*

- This covers the one time exemption for 24 months for newly identified CCAs at newly identified CAs – everything else is consistent with existing effort.
- Is implementation the appropriate word? Good intent but is it the right word.
- Still need to factor in 706b and when to file TFEs
- Not changing the newly identified CAs – just a one shot in this particular table
- The other implementation plan is already approved and this represents a one shot /one time exception. Not changing the plan but providing a one-time override? How does this play with the new CIP 005 version?
- Does this cover the need for outages to implement?
- It gives them 24 months to incorporate
- In theory the existing plan did not include that either, this gives more time.
- If not changing plan, do we have flexibility to just say 24 months to give people a clear date?

- Today I have zero time for something new – if build something new, do I have 24 months from commission?
- If did not plan for it to be CA but not online yet but will be a CA once commissioned.
- Suggesting 24 months to bring everything into compliance.
- Concerned if some of us are still confused – once turned over to NERC regions, they may interpret differently – needs to be spelled out as simply as possible to limit the potential interpretation confusion
- Second paragraph – next subsequent application is July 2 as part of update as needed – may need to clarify it is the next annual application, not the "as needed during the first year."
- How do you handle a new CA going into service within the 24 month window – if building it now

**Straw Poll on Proposal**
**Favor proposed approach to drafting implementation plan**
**Yes=9 Oppose=4 Abstain=5**

**2. Alternative Approaches to Developing the Implementation Plan**

Following the poll the SDT identified and discussed the following potential alternative approaches:

a. Implementation plan that requires identification of CAs within 1 quarter and CCAs in 4 quarters. Existing Newly Identified CCA Plan could be used (but the clock would not start for these new CCAs until 4 quarters (12 months) after approval

*Or*

b. Develop a new implementation plan that allows
   1. 24 months for Newly Identified CCAs and New CAs and
   2. Uses the existing Newly Identified CCAs for New CCAs at existing CAs
   3. Keep the newly identified CCA

*Or*

c. Add one quarter to Scott Mix's original plan for effective date.

*Or*

d. Develop a one-shot/one time exception (for specific circumstances) with a sunset to the existing implementation plan schedule.

*Or*

e. Provide six months for identifying and 24 months to comply.

*Member Discussion of Potential Alternatives*

- Don't remember modifying process in 002 to identifying CCAs. The proposal did not modify the definition.

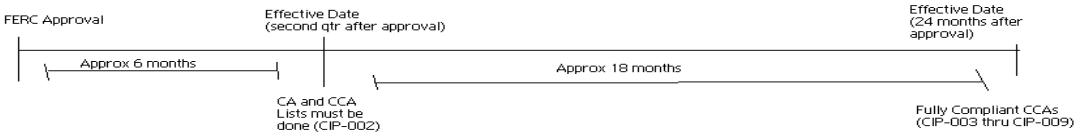
- **Alternative a.** gives a window for plant that does not have a plan.
- in #1 does it buy any time – concerned most about CCA list and identifying when that list has to be in place – having it on the CA list does not necessarily mean it will have CCAs
- **Alternative b.** gives entities time for newly identified, not existing identified assets.
- It uses existing criteria.
- Has to be compliant on day one
- b1.? Does this override one aspect or mean change approved document –
- If 10 and 11 comes in the middle may create issue of overlapping schedules
- FERC staff is nervous about opening up the implementation plan again – would the simple answer be that non-nukes use one plan and nukes another – with exception for more time in specified circumstances?
- Need to leave nuclear open – may come up with a procedure approach
- Concern is mostly about generation rather than transmission? Several transmission stations will also be brought into the mix
- We could move forward with what we have with an addition for exceptions, or build time up front
- What is the time frame for CA and CCA identification and then the time for implementation – when does the race start and how long do you have to finish
- Abstained from the poll because I do not have assets at risk.
- Might also consider from an audit enforcement perspective
- If we do not want to open the implementation plan up then b. and e. are out
- Don't like 24 months which bumps up to the next version and will not fly optically with regulators
- Implementation plan should use the IPFNICCAANRE as it currently exists
- Whatever we use, the visibility is critical to show moving forward on implementation – i.e. a plan that shows we are moving forward with visible dates that can be easily understood.
- What about 18 months? Consider possible TFE for shut down issue?
- Whatever is proposed will need to be justified. It will be easier to justify if tied to something already approved by FERC.
- There seems to be agreement on the concept but we haven't settled on the length for compliance.
- Implementation plain remains as is with a one-time one-shot exception for 18 months, Alternative d. The other half is when to fire the start gun – six months?
- What benefit do we get from all this rather than go with existing plan? Build in buffer
- Use existing implementation plan with process for exceptions if need more time
- Putting in an exception process may take long time to get through legal.
- NERC staff needs some words to take back to compliance director and legal department to see if we can put that into the implementation plan

- Keep in mind time is short to reach agreement on everything to be posted following your September meeting.
- This is offering a one time shot exception – first application of bright line
- Adding in "compliant at 24 months from identification" helps.
- We are talking about CIP 002-009 not just CIP002.
- Should be a date legislators can easily understand and see.

**Proposal:**

**For the initial application of the "bright lines" in CIP 002-4, CCAs at newly identified CAs will be compliant at 24 months from identification (add 706B items and TFEs)**

**The effective date of the standard (upon the regulatory approval) the registered entity will need to identify CAs and CCAs within six months and xx months to be compliant with 003-009**




*Discussion Comments*

- Effective date is the date FERC approves? It is based on the approval
- There is the issuance date and then effective date. Effective date is the day after auditor can ask for compliance – the date you must have a list with signatures.
- We are looking for the list six months after FERC approval, then 24 months to bring into compliance.
- Move away from the number of months and be sure we have the concept

The Chair and Vice Chair thought there was enough input for a drafting team to develop a new proposal and solicited volunteers for a drafting team to bring back for the SDT's consideration in September.

**Implementation Plan Drafting Team Volunteers**: Sharon Edwards, Dave Revell, Kevin Sherlin, Scott Rosenberg, Mike Keene (FERC), Dave Norton and Phil Huff

## Appendix #8- CIP 010 & 011 Sub-Team Proposal *(Phil Huff)*

**Proposal for Sub-Team to Develop Foundational Principles of CIP-011**
*This proposal was initially presented on Tuesday and discussed in greater detail on Thursday.*

The process for the informal comment posting provided little time in developing foundational concepts to applying security controls and industry guidance. Drafting sub-teams must make decisions on applicability according to impact, connectivity and operating environment, but they do not have a common basis for doing so. As CIP-002-4 lacked technical justification for bright-line thresholds, so now CIP-011 lacks a solid basis for determining whether or not a security requirement is appropriate.

**Proposal**
Form a sub-team to further develop concepts in presenting and scoping cyber security requirements for CIP-011. This would include the form of CIP-011 and basis by which sub-teams write and apply requirements. This would NOT include the actual development of security requirements.
Ideally, team members not heavily involved in the drafting of CIP-002-4 could contribute to this effort. The output of this team would go before the full-team for review and approval once CIP-002-4 has been successfully balloted. The objective of this sub-team would be to further develop concepts in CIP-011 and improve the efficiency of CIP-011 sub-teams.

**Issues to Consider**
- Impact – what types of security requirements apply at what level?
- Connectivity – How does connectivity factor into applying security requirements?
- Operational Environment – How do different operating environments factor into applying security requirements?
- Type of System Considerations – How do types of systems factor into applying security requirements?
- Technical Feasibility Exceptions – Propose an improved process to allow entities to apply appropriate controls while still satisfying the requirements for transparency and oversight.
- Format – Technically present the Standard in a way that communicates to owners and operators of the BES

**Deliverables**
- CIP-011 Format Proposal
- Guidance/rationale preamble to CIP-011
  - Description and basis for scoping filters
  - Guidance in reading the CIP-011 format

- Proposal for Technical Feasibility Exceptions

**Timeframe:** December 2010 Meeting

**Appendix # 9 SDT Discussion Notes of CIP 010-011 Schedule and Approach**

*SDT Member and Participant Comments*

On Tuesday the SDT reviewed initially with Allan Mosher the proposed CIP 010-011 schedule and approach. On Thursday, the SDT took up the review of the schedule and tasks for completing its work on the CIP 010 & 011. Phil Huff reviewed with the Team the key highlights of the draft schedule:

- First posting for Formal Comment is proposed for May 31, 2011.
- This assumes an aggressive NERC industry communication campaign to support the effort prior to posting for formal comment.
- By December the SDT will turn its full time attention to CIP 010 & 011.
- By March the SDT will send a package for review with NERC staff, compliance and legal.
- Review in April any edits and Approve in May.

*SDT Member and Participant Comments*

Stu Langton suggested there was an important discussion of three distinct issues: schedule; preliminary work on next phase; and deeper issue of approach to drafting during the next phase. We may need someone to work on and present a suggestion on the drafting approach for the next phase in Winnipeg.

**Schedule & Industry Confusion and Communication**

- If we ballot on this schedule and approval in 2012 – period of 2012-13 will be confusing for compliance – anything in this schedule help smooth this for the industry.
- We will be hitting them with ballots just when 002-4 becomes effective
- FERC staff expressed concerns about how aggressive the schedule is – still talking about a draft ready for compliance and legal review by March.
- Howard Gugel noted he is reaching out to communication manager to develop plan – considering series of webinars that look at key components with more focused discussions.
- Are webinars being designed as a one way or two way information process? Allow informal comment or feedback mechanism in the webinars. Once in the ballot phase, it is more difficult to change – you are a representative body of the industry – informal comment lets you hear from the industry and gives you a chance to fix it – need better feedback mechanism from industry.
- Concern with the schedule – did not see any milestone for dealing with inertia of the response to CIP 002-4 – switching back to 010-011 may be a big issue and

difficult sell to industry. Didn't see that dynamic noted in the schedule. As of today, not sure the team is fully behind the change to 010-011. We will need the SDT to come together and a convincing communication plan with the industry of the value to moving toward 010-011.

**SDT Deliverables- Short and Long Term**

- April 1 is the date that sticks out – that is the last day before turning it over to NERC staff? This version has built in three reviews with the NERC staff.
- This may be aggressive but we have not fully defined the concept. There are bigger issues than just revising standards.

**Sub-team Setting Out Proposed Approach for Full Team SDT Review.**

- Phil Huff noted he wanted to propose getting a new sub-team to work on material issues between now and December, for example, impact, connectivity, operational environment, type of system considerations, TFEs and format. It could deliver CIP 011 format proposal, guidance and preamble for 011 and a proposal on TFEs for review at the December SDT meeting. They would not look at requirements.
- Understand concept but may also need to consider the overlap of new CIP 005 team. Also heard concerns about potential overlap with 002-4 implementation plan and how aggressive that schedule appears.
- The concept is good idea to compensate for the divergence of CIP 002-4. However still concerned about the fragmentation of the SDT. Once we come together in December we need to reconsider the model of using sub-teams. WE need to go through the requirements as a full team. The results of the proposed effort could give us a start – let this sub-team take a first cut at requirements and house keeping, then starting in December we should focus on full team review given the aggressive schedule – need momentum – feeling numb and disconnected by the current sub-team approach.
- We will need to continue to make changes between meetings – may need to continue a sub-team after December to get pen to paper. The proposal is not to break into subteams during SDT meetings and anticipate full SDT review of work done between meetings.
- Consider using full team webinars between meetings after December.
- Suggest functional areas be assigned for expert drafting to pull together into a strawman that all can review in calls and full team meetings.

**SDT Organization in 2011**

- As an observer, it appears that the team is good at policy but not at putting pen to paper – use the SDT as a policy group and hire someone to draft the first draft for review by the full group.
- In Sacramento the SDT discussed the need for time. The resulting deal was to work on CIP 002-4 now to December then take another year for 010-011. This draft schedule does that by working back from December 2011 delivery.

- We need to develop and review a more detailed schedule in terms of making sure the resources available. WE cannot manage this project at such a high level of generality and be assured of success.
- We should clarify and adopt clear guidelines for any subteams going forward. Sub-team assignments should be made clear in terms of what to produce and when return to full team.
- Tuesday and Wednesday's work on CIP 002-4 were very productive for this team – everyone understood how we got there.

**Overall Approach to CIP**

- Dave Norton offered the following thoughts for the SDT to consider in thinking through its schedule for the CIP 010 & 011.
- We are searching for elegant language that covers everything – do not think it is possible to write language that covers our legacy assets and anticipates all the coming changes and challenges. Our product needs to be amenable to changes we have not even seen –
- Our friendly regulator is concerned that we have written one requirement that applies in a binary way based on the size of the iron and not on the risk based approach of NIST which applies no matter the size, then adds more specific language for specific challenges such as data centers. FERC staff urged us to have base layers and add specific requirements for serial, wireless, routability, etc.. That is, protect bastions with physical security, but parse the problem – not one issue with a binary solution. If we don't do this, NERC should expect to face remand.
- Our largest organizations, IOUs, have a weighted impact in terms of ballots as they have the largest investments in the most complex programs, policies and compliance programs in place that have been oriented to the existing 003-009 categories. They are not happy about putting it all into a single 011 standard. Access control is an example.
- The SDT also needs to address "defense in depth" – there is network defense and host defense – more elegant to address access control holistically but most in industry are not prepared to do so. There is a fear that industry will vote it down because they don't like it. An incremental change would be to use the current structure and build off of that.
- 33% of requirements apply to low end is a challenge for FERC review. We need to focus on routable as the vector that needs the most protection – regulator doesn't like 011 and industry doesn't like 011 – schedule is relevant only to extent you identify the path.
- Politics not addressed are the quality of the product you put out – bad optics if industry rejects but almost as bad if you are simply self-reporting constantly – this is too complicated not to have a base for discussion and editing – too long to argue over every word – need to run this as a project – fix it right the first time or just do 706 in the 003-009 frame.

- Have to break this down – this is only drafting team that has to formally use tents – originally intended to break this group into multiple teams – many say they will never create a team this big – cannot solve this problem with everyone sitting in the room – have to have teams break off and use ballot body to comment.
- The question is whether 011 is the right product in FERC's view. There are two core problems with current 002 model: 1) the initial mistake to eliminate the communication links which has now have created islands and failing standards. You don't know what you are protecting – in federal framework we are protecting base and work from there – working backwards from sites and assets. We need clarity on what we are protecting – fix what we are protecting. We may be on the wrong path and facing remand. We haven't clarified what are we protecting against. We have to move to a new model.
- Clearly, as a team, we have problems with the underlying concepts for some on the team, but that doesn't mean we should just scrap work to date. There are still some key questions for team to work out before jumping back into the requirements. Yet we still need to provide a schedule.
- Is the team ready to agree on a schedule? If we don't know what we can deliver how can we know when.
- We've heard and had the same arguments before regarding approaches.
- After robust debate, we agreed on the concept and worked on it. We are now close to where the whole team can work on requirements. All this was forged through a stringent voting requirement that got us to this point. We should consider whether to move on to finish the product or scrap it?
- We are still not looking at security protection and industry view. The major driver is keeping the financial cost and risk low – not on what should we be protecting.
- Cost, however, is a legitimate part of the SDT's consideration.
- We don't know what it will cost in a risk based system.
- We should focus on 706 orders and incremental improvements in the past – but is the product out of date and do we need something completely different? What we have today does not address the problem. We may need to build a new product that works – redefine the problem before we can set the schedule
- Members have to make proposals and if it does not get team support then you have to move forward with the team. It is good to discuss and test these, but we have to move forward as a team – once argument is made and then direction chosen then have to move forward.
- FERC staff: Mike Peters speaks for himself, not the FERC commission or staff – staff and commission said the NERC/SDT should create a baseline then consider specialized protection as needed. CIP 011 is a step in the right direction to applying appropriate protections to different levels. There is no reason the CIP 011 structure cannot fit. One statement cannot fit all – what it is, where it is and how it is protected. I think team can do it, has been productive in Pittsburgh and here in fleshing out Attachment 1 which was, by the way, drafted by a small group. Our

observation is that the small group approach is a valid approach as long it comes back for review, refinement and adoption by the SDT.

- Need to attack our task ahead as a project. We have had no one place to draw on as a source. CIP 003-009 can still work as a base or root stock and we can apply the sub-team work to that frame, use 706 to provide incremental improvement – and we can absolutely make it work by mid year.
- Team is split into I.T. and power engineers – problem in philosophy and finding a mutual mid point we can agree on.
- Take what we have and fix based on 706 request – two glaring issues with current: doesn't cover enough and doesn't cover communications. We are working on the former with CIP 002-4 and the latter can be added by this group. We can do it, it is aggressive but doable. If we don't in six months it will be taken away from us.
- We keep working through different perspectives and appreciate each others talents – still think there are foundational issues that a sub-team can look at between now and December to give us the starting point.
- We have some issues – sub-team needs figure it out and then six months to work as full team
- In Sacramento we said March was doable. With the CIP 002-4 delay, I think that May is doable
- From NERC's perspective, there has been a considerable investment of money and time in developing consensus around 011. The SDT was then were diverted from outside. The SDT needs to decide if investment can be applied to create value. You need to give us a schedule on a solution not just CIP 010-011. You need to ask yourselves if CIP 010-011 is the right approach, and if yes, then go forward and bring it to the industry. If not, then the SDT needs to develop an alternative plan and get to the job.
- Feedback we are receiving from industry to posting is that the High/Medium/Low represents a significant change. Regulators seem to say you need a baseline to build on. Appears that the industry and regulators are at odds and team is trying to walk the line and please both. Taking away 003-009 was too much for industry to digest. Learning to making changes to 003-009 based on 706 – from day one with this team we developed camps about protecting systems. Somehow we keep coming back to feeling among some that the validity of there position has not been addressed.
- This is the elephant in the room – keep 003-009 or come up with a new solution – if we have a quorum, lets decide and move forward.
- We have a target audience and regulators with different expectations and the SDT is between a rock and hard spot – trying to build a consensus between big iron and systems – need to tailor approaches up from a base up, not a top down approach because we continue to get different results from the two models.
- We did vote on the concept, and with less than the 75% support decided to go with 010-011 in order to get the industry comment, refined and got simple majority again/

- Thought we got over hump of the systems approach – don't quite get if we apply 10-11 approach, where are we missing the point, a flawed approach?
- The substance in CIP 011 is not wrong but what is the gain? Is it cosmetic only?
- To clarify issue. If what we have in 011 today is wrong in terms of its content, then we have a threshold issue and problem. On the other hand, if it is the issue of format and having it all in one standard, that should be much easier issued to resolve.
- Concerned about motions and deciding this evening. The proposal to form a team to look at this was a correct approach. Its like we voting against taxes and then asking a team to develop a tax plan.
- In discussing the schedule we didn't start by figuring out requirements and resources then agree on a schedule, instead we have been told what date will be done. However we need to take the date seriously or the job will be taken away not just from the SDT but from the industry.
- The SDT is still not discussing what to protect – format is not substantial issue – we do not have glue between 010 and 011 – still don't have an approach to controls – break up controls based on how they are applied, not by the existing standards – if whole new paradigm then break them out – schedule is good because we do not have any choice
- FERC and congress would be happy with control centers and protect BES and be done. continue the CIP 002 approach that leads to a test program. We worked on and got super majority (75%+) on not using CIP 003-009 structure. There was simple majority support on 011, important concepts in there – naysayers continue to wait and continue to revisit – we can't go back to what we have. However, not in favor of a yea/nay vote today.
- Is there problem with the work on 011 so far? I am pleased with much of that work – keep in mind how far we can move the industry and still move toward the objective – do not want to lose that work, still needs to be vetted – I voted against 010-011, but as a team player I support moving forward and retain good work so far.
- We have power plants that do not affect the system – we would shut them down rather than spend the money to protect them – unintended consequence of protecting everything – some equipment doesn't need to be protected – ask industry what they think – you asked them a million questions and got a million answers –
- FERC staff perspective: industry and regulators may sound like opposites, but not sure that is true. The problem may be more about how to write these concepts into the standards – much of your work facilitates getting the basics out there. John Van Boxtel's format model may offer unique opportunities as the tables did not have sufficient detail. His model proposed making the tables the minimum and then look at extra schedules for specific elements. The SDT is poised to make a necessary paradigm shift to a protection culture. O10 & 011 are looking for protections of assets appropriate to the risk of reliability of BES with appropriate

controls to be applied to address risk to BES. It is less important if in one clump or separate pots.

- My urge for a motion today is just to move forward is born out of frustration of revisiting issue at end of a long day. In Atlanta, we did have super majority (75%) to abandon the CIP 003-009 going forward and we made that call despite industry reaction. The separation of transmission, generation and control centers is not the issue, rather it is the control systems across all of them. The technology based system controls are the issues we need to look at, but we are being told, and have agreed, to provide in the interim a bright line that not a risk based system.
- The SDT was put together to address order 706 and to look at and consider NIST as we modify existing standards based on 706 as a base for future changes. We decided to go to High-Medium-Low. The industry may not yet be ready for a change.
- NERC staff is facilitating rather than managing. Maybe we need to manage, first nail down scope – we have been subject to "scope creep", of plan B and multiple versions to address outside issues. We looked at the structural problems presented by multiple standards and chose to move toward combining into one. We still need a common lexicology too – we should focus on function technological system approach – on h-m-l looking at control systems. Congress does not distinguish between different systems whether corporate, market or control systems . We need to move toward a result based system – compliance and fear of costs is currently driving our process. Going back to to CIP 002-009 will not solve the problem. The industry's comfort with the old system and the sunk costs should not drive our process.
- Many of these comments highlight the issue of communication with the industry – much higher potential for external entry from a connected 25 mw unit than an older 1000 mw unit without connection – communication allows you to tunnel to fifty sites – it is about the control, not the size of the unit.
- So the result may be that the weak link will be shut down as not economic and you may have just degraded the reliability of the network and the grid.
- Some things being proposed still fit into the existing system. We have disagreements on approaches and formats but there has been good quality work to date.
- Back to the discussion of the schedule the proposed schedule on the table to post 010-011 at end of May and passed by end of the year by Board of Trustees

On Friday morning, John Lim reminded team members of importance of working together as a team. He then withdrew his motion on the CIP 010-011 schedule from day before for sake of offering another motion that may be clearer and reflect the good discussion points. Phil Huff noted he will put two motions forward that will describe a process for moving forward on foundational concepts discussed yesterday. The motion moves the posting date for formal comments back to July, 2011 and suggests taking time in front end to set foundation before launching into the requirements in January 2011 providing three more

months for the foundation discussion. Phil Huff made the following motion which was seconded by Dave Norton:

**1st Motion for CSO706 SDT Project Schedule**

The CSO706 SDT will prepare a complete package for initial posting to the industry for consideration and ballot in July 2011, in response to FERC Order 706, ~~including the requirements, implementation plan, guidance documentation, and other related documents and~~ with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without major redirection of SDT efforts. ~~ancillary assignments.~~

**16 in Support; 1 opposed (94%)**

- Concerned regarding the management of the Team's effort moving forward

*Discussion of Motion*

- Finite amount of time – before setting out on work take a check point on where we are – a check point restart
- Agree need to review but concerned about targeting completion in middle of next year – resources set for this effort, schedule set, then only thing to adjust is scope – seems a little backwards
- Concern we do not know where we are going and are setting a date – don't know yet what success looks like – make industry happy or the government.
- Politically and optically we need to deliver timely or this process will not exist – time and resources are finite
- We said we would do it right – responsive to 706 and industry – we can put package together by July but not FERC by end of year – we don't control last half of the year.
- Have to deliver something. This is a reasonable motion to move us forward.
- This is not throwing away all the work to date – but still foundational issues to tackle – this reflects time to do that.
- Two paragraphs are tightly linked – need foundation set by December – also concerned that this hits at same time 002-4 adopted in mid summer.
- Why pick a date before we know what we are going to do? Standards Committee requested a date for completing the project – may know better in December the actual date.
- We took a year to do other work – then hit by "plan B" by end of year – that is why we are dealing with this – now they want a stake in the ground for completion – we should focus on 010-011 (if no more curves can we finish?) – Yes, but concerned that 002-4 will set industry into its ways and bolster opposition to 010-011.

- Do I think team can meet July deadline? Yes but we have to educate the industry with a communication plan before presenting for ballot?
- I can provide my time as necessary but what is the scope and time demand on members – a yes vote is a commitment to make this happen – can others meet that commitment.
- Need to provide by end of 2011 – 002-4 will further entrench current methodology – concerned this proposal will support return to 003-009.
- Does not mean we have chosen which direction – second part of motion says we will look at direction – sub-team will not be looking at 011.
- Are we freezing 003-009 in place? Uncomfortable with that possibility.
- Look at language offered here and IT seems going back to earlier discussions of format – are we going back to revisit that? Implying 011 does not stand, revisiting the issue?
- Phil Huff noted that was not the intent. Not about redeveloping concepts but there are many we have not looked at yet.
- Looked at catalogue and developed concept – language here implies sub-teams rewrite sections – some here think fractious conversation is due to lack of full team review – resetting in January?
- If commit to dates and SC. They must make a commitment not to throw us any more curves. Recount to them how many diversions they have made for us. They need to leave us alone to do our work – bilateral commitment.
- Second issue – why take until December to line up our ducks – I volunteer to lead it in two months.
- We have to respond to comments to 002-4 – December the first chance to devote full time to the next stage. We may have time in October to look at it too?
- On the second motion – sub-teams have come back with different formats and content including factors on controls – need more uniform method of targeting those – not redoing the controls but improve targeting to hit those most important.
- July is the team's concern – after July it is on NERC and industry trade associations – critical for NERC to educate the industry on the concepts for industry support. Team can produce quality by July and fails due to lack of communication then that rests with NERC and industry trade associations. We can deliver quality product for industry review in July.
- What we are doing about 002-4 now? What is the communication plan for that? There is confusion in the industry as to what we are doing and why- the ask what happened to 010-011, also, risk to schedule is March 31 response from FERC on 002-4 that asks us to do something else with it.
- Concerned about filing to FERC by end of 2011 – make it "with the expectation of ballot body approval and filing to FERC …." – we control up this up to July, 2011.
- Put period after July 2011 then new sentence: "This schedule would provide the industry with the opportunity to …"
- PH – concerned about the last suggestion – still part of the schedule even if not in our control

- Still responding to the formal comments – prefer "with expectation"
- Complete package implies the subparts will be included – "initial posting to the industry for consideration and ballot in July 2011 with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without any ancillary assignments.
- Concern about setting end date you do not control if FERC asks for more in March
- Language assumes FERC does not ask for any additional work on CIP 002-4.
- Question about assignments and distractions – need to include communication or NERC leadership on what we are doing and going – turbulent waters will get muddy in January when CIP 002-4 is posted, also say we want communications that have been missing.
- NERC hears this loud and clear but this team cannot dictate. If this team produces a standard proposal in July, 2011, the ballot body approval will not happen without communication. Communication does not impact team's work but assignments would.
- If additional risks pop up, we should assume it will throw us off schedule.
- Keep struck words referring to 706.
- We know what ancillary assignments are but will others – "without additional major redirection of teams effort."
- Last time it was a request to redirect not an ancillary assignment
- Sounds a little catty – we accepted last assignment and did it and rescheduled
- We have become a standing committee on anything cyber – yes, nested and have to hang together – but this group is not the normal approach to standards development – let us finish before giving us anything else – take out additional to avoid catty?

Phil Huff proposed and Dave Norton seconded a second motion (second paragraph)

**2nd Motion Process for Implementing CIP 010-011 Schedule- Framework Sub-Team**

The CSO706 SDT will form a sub-team to develop a framework for presenting and scoping cyber security requirements for preliminary delivery in October 2010 and completion in December 2010. This would include the form of the standards and the basis by which the requirements are written and applied. The output of this team would go before the full-team for review and approval. This task would not include the actual development of security requirements.

*In Favor of the Motion*
**Yes=17 No=0 Unanimous**

*Member Discussion of the Motion before the Vote*

- Agree with the intent it should be clear to those writing the requirements as to how to write them. Go together as a framework that will need joint discussion. The Sub-team should take an initial stab at writing initial requirements.
- Should it take it to point of filing in the blanks? By October should present the direction to the SDT and then finalize in December. Cut and paste what we have and let full group redirect in October and December as needed
- Concerned about waiting with the current Sub-teams. We cannot afford to wait – would continue subteam work on requirements then full team review –
- Drop "sub-teams" and just say "by which the requirements are written and applied."
- This proposal draws on the essence from Phil's first proposal (*See Appendix 8)*. Much of that detail is in the original to set framework for hanging the requirements – it offered specific suggestion of issues to look at from our earlier questions – something of a quality check-list.
- We need to talk about the fundamental framework and logic for attacking the requirements. –A style guide is a good description but may need some refinement first.
- Concern with first half – we often break down when concepts brought back to full group an get lost in the woods of word-smithing deferring the more foundational discussion which now must happen in order to set our core message.
- Specific deliverable for this Sub-team should not be a concept paper. Perhaps it should say framework. A**c**cept amendment for framework instead of concept
- Intent is to "develop a framework" not "further"
- The intent is it incorporate and not disregarding the raw material have worked on to date – preliminary delivery in October to the full team and presentation to the full SDT in December for refinement and adoption.

The Chair asked for volunteers for the Framework Sub-Team and the following members and participants responded.:

- Dave Norton (Lead)
- John von Boxtel
- Joe Doetzl
- Dave Revill
- Doug Johnson
- Phil Huff
- Jon Stanford

Other volunteers included:

- Mike Keane
- Scott Mix
- Joe Bucciero (Facilitator)

It was agreed that Joe Bucciero would send a note to those members of the SDT not present asking for others who might want to volunteer

Following the vote the SDT agreed on the following direction to the current CIP-011 Sub-Teams: We need the output from the sub-teams on responses to industry comments and workshop comment summaries so they can be posted in October and recognize industry's investment into those comments.