NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

29th Draft Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Orlando, Florida

December 14, 2010, Tuesday - 8 AM to 6 PM EDT
December 15, 2010, Wednesday - 8 AM to 6 PM EDT
December 16, 2010, Thursday - 8 AM to 6 PM EDT

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

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

CSO706 SDT December 14, 2010 Meeting Summary Contents

Cyber Security Order 706 SDT- Project 2008-06
29TH MEETING
December 14-16, 2010
Orlando, Florida

EXECUTIVE SUMMARY

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Orlando and thanked member Rich Kinas at Orlando Utility Commission for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Wednesday morning, the SDT unanimously adopted the November 16-18, 2010 Baltimore meeting summary. The chair outlined the objectives the SDT sought to accomplish by the end of the meeting that included review of and agreement on the response to industry comments as well any changes to CIP 002-4 and its related documents, initial review of strawman documents from the Framework team and training on results based standards development.

The Chair reported to that Team that the successive industry ballot on the CIP 002-4 received a quorum (86%) and received 77% support of the industry which was a significant improvement from the support for the first ballot (43%). Howard Gugel, NERC, reviewed the revised comment process clarifying the distinction between a successive ballot and a recirculation ballot. He suggested the SDT should consider and weigh whether any changes in the standard would help change a "no" vote to a "yes", would help to retain the "yes" votes, and keep from turning abstentions into "no" votes. He explained that the successive and recirculation ballots are part of the ANSI process intended to everyone give chance to reevaluate their votes based on the Team's clarifications and answers.

Gerry Cauley addressed the SDT by telephone at the beginning of its meeting. He started by congratulating the team for its hard work under pressure and in responding to his request to bring CIP 002-4 to the industry for balloting in 2010. He noted it has proved useful in discussions with Congressional staff and has had a positive impact on NERC's reputation and credibility in terms of standards development. He clarified his thinking on the path forward for the Team, consistent with its SAR in addressing the FERC Order 706 directives. He suggested that it might be possible to address those directives in the CIP 10-11 framework the SDT has been developing or within the CIP 003-009 framework. He noted that many CEOs have expressed to him concerns about shifting away from CIP 003-009 and the documentation necessary for compliance, but stated that it is up to the Team under the standards development process to bring the proposal to the industry for comment and balloting.

He reviewed his comments to CIPC the past week which he characterized as exploratory in terms of consideration of a more coordinated and comprehensive approach to the goal of security of the BES among efforts such as the CIP standards, the NIST smart grid initiative etc.. He noted he is considering possible approaches including putting together a team that might, in partnership with NIST, address this broader concept and that might lead to a comprehensive set or suite of voluntary "good practice" security guidelines over several years of work. In response to questions, he noted that the SDT needs to address directives and chose which path or framework, in consultation with the industry, is best for reliability and industry implementation. Getting CIP-002-4 will be a first step along the path and NERC will continue

to support the SDT efforts. For the foreseeable future we have to finish the SDT's efforts to address the FERC 706 directives. This other best practice guidelines effort is more long-term with the hope that over a few years we can develop consensus on a voluntary tool kit that will not replace the standards. We will have to wait on experience in developing the guidelines before moving towards any corresponding standards development. The Chair thanked Gerry Cauley and he thanked the Team again for its hard work. On Wednesday afternoon, the SDT discussed Gerry Cauley's comments in relation to future CIP framework for the Team. The comments focused on completing the Version 5 work and clarifying the nature of the parallel process Mr. Cauley outlined.

Scott Mix provided an update on the recent ballot for updates to CIP-005-4 regarding remote access. The ballot concluded with an 84.46% quorum, but a 42.89% approval rating. Approximately 100 pages of comments were filed from both the comment period and the ballot process. The team will be meeting to start responding to comments and modifying the requirement in response to comments. Mr. Mix is also looking into whether a Compliance Application Notice (CAN) can be written to address some of the "double jeopardy" issues identified in the comments (i.e., indicating that some "global" requirements in existing standards will need to be applied to remote access if they are not already). The desire is for the revised standard to be passed by industry and be submitted to FERC in time for the commission to act concomitantly with the CIP-002-4 action. Failing that, the guidance document developed for the standards revision will be handed over to NERC staff for posting as a document in support of the FOUO VPN Alert, and the standard requirement and industry comments will be turned over to the 706 team for its deliberation and consideration in the future version of the CIP standards.

Scott Mix noted that the CAN 005 Remote Access has been noticed as withdrawn and would be undergoing revisions and then reposted.

Howard Gugel reported that the successive ballot of the Cyber Security 706 CIP Version 4 standards was conducted from December 1-10, 2010 and achieved a quorum of 86.83% and a weighted segment approval of 77.04%. Howard provided information on the difference between a successive vs. a recirculation ballot.

During the course of the three-day meeting, the SDT reviewed each industry comment and considered and refined strawman responses and agreed on final responses and on any changes to the standard documents. Each response was either unanimously agreed to by the SDT or the level of consensus was tested with the use of straw polling that helped direct refinements that built sufficient consensus (i.e. support of at least a 2/3's of the SDT members). Below are the key straw polls that lead to refined responses.

On Thursday morning, the SDT, following input from NERC Counsel, moved *(Tom Stevenson with Doug Johnson as 2nd)* to accept the proposed nuclear language with the motion carrying unanimously. Following that, the SDT moved *(Sharon Edwards with Bill Winters as a 2nd)* to approve the package of CIP 002-4 documents (including, Cyber Security — Critical Cyber Asset Identification CIP 002-4, Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4, CIP-002-4 Rational and Implementation Reference Document, Consideration of Comments on Successive Ballot for Cyber Security 706 – CIP Version 4 Standards, and Consideration of Comments on Project 2008-06). The motion passed 17 - 0 with 1 abstention.

Phil Huff reviewed the work of the Framework Team since the SDT meeting in Chicago in August. Since the Baltimore meeting the Team has developed a strawman meeting schedule, a style guide, and a communication plan.

In terms of the overall schedule, Mr. Huff noted that the SDT will begin next month with a possible posting late June or in July. The Framework Team believes that continuing with a sub-team approach may not be the most effective way forwards. Instead they are recommending drafting assignments to Team members and utilizing the full team monthly meetings to review and refine strawman drafts.

The Framework Team has developed a "Style Guide" for drafting results based standards. The Framework Team is recommending a BES cyber system identification using several impact levels: A (high) and B (medium) and a baseline level for low. Part of the communication plan that NERC will work with the Team to implement will include a change document providing rationales for the proposed changes and mapping back to the existing CIP structure. Where possible the existing structure will be retained and justification will be provided for changes are needed. The following are the SDT areas of discussion of the Framework: Clarify Format and Organization; Clarify Proposed CIP 11 "Organization Requirements; Clarify How Many Levels of Impact; Clarify the Scope; and Consider Independent Certification Process.

In preparation for the Version 5 drafting challenges, the SDT engaged in a results based standards review and training conducted by Keith Heidrich FRCC, on Thursday of the meeting. Mr. Heidrich has participated on an ad hoc NERC team convened by Gerry Cauley which has been developing the concept of a results based standards approach. The training objectives were to: Identify and give examples of the elements that define a results-based standard; Analyze the current standards and requirements for weaknesses; Identify the needs, goals, and objectives for this; Create an initial draft of this standard and requirements using result-based methods; and Create measures and necessary supporting material for the standard and requirements. The training covered: Results-based standards/requirements – what are they and why they matter; Scope–what you need to know before writing requirements; Standard requirements – observations and improvements; and Where information is recorded – templates.

On Thursday, Phil Huff noted that based on the review and discussion at this meeting the Framework team would be proposing two impact levels with all other being those items falling outside BES system definition. The Team will present a refined proposal in January taking the SDT input into consideration. For those in those covered in one of these two levels there will be multiple types of controls to be applied. It will get down to the drafting requirements in a consistent format. We recognize detail still needs to be worked out.

The Chair and Vice Chair noted that the expectation is that following the January session the Framework Team would dissolve and an open set of SDT meetings will be used to refine the proposed framework through review of strawman drafts of requirements. The Framework Team will set up conference calls in January in advance of the Columbus meeting.

The Team reviewed the steps and assignments leading up to the Columbus meeting. The Framework Team will be meeting in early January 2011 to prepare documents for the SDT to review at the January 2011 meeting. The recirculation Ballot is expected to close on Friday, December 31 COB. NERC staff will notify the SDT of the ballot results. The Chair thanked Rich Kinas and the OAS for the hosting of the SDT in Orlando.

The meeting adjourned at 4:40 on Thursday, December 16, 2010

Cyber Security Order 706 SDT- Project 2008-06
DRAFT 29TH MEETING SUMMARY
December 14-16, 2010
Orlando, Florida

I. AGENDA REVIEW, WORKPLAN SCHEDULE, REMARKS AND UPDATES

A. Agenda, Milestone Schedule Review

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Orlando and thanked member Rich Kinas at Orlando Utility Commission for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Wednesday morning, the SDT unanimously adopted the November 16-18, 2010 Baltimore meeting summary.

The chair outlined the objectives the SDT sought to accomplish by the end of the meeting that included review of and agreement on the response to industry comments as well any changes to CIP 002-4 and its related documents, initial review of strawman documents from the Framework team and training on results based standards development. Bob Jones reviewed the timed agenda which included reviewing ballot and comments on Tuesday, look at remaining 706 directives and the framework effort moving forward on Wednesday, and engaging in a training effort for members on result based approach on Thursday.

B. Overview of the Ballot Results

The Chair reported to that Team that the successive industry ballot on the CIP 002-4 received a quorum (86%) and received 77% support of the industry which was a significant improvement from the support for the first ballot (43%).

Howard Gugel, NERC, reviewed the revised comment process clarifying the distinction between a successive ballot and a recirculation ballot. He noted that if there were significant substantive changes made in Orlando, it would require a new ballot process. He suggested the SDT should consider and weigh whether any changes in the standard would help change a "no" vote to a "yes", would help to retain the "yes" votes, and keep from turning abstentions into "no" votes. He explained that the successive and recirculation ballots are part of the ANSI process intended to everyone give chance to reevaluate their votes based on the Team's clarifications and answers. The Team will need to draft responses to both the negative and positive comments.

C. NERC CEO Gerry Cauley Remarks to the SDT on Cyber Security

Gerry Cauley addressed the SDT by telephone at the beginning of its meeting. He started by congratulating the team for its hard work under pressure and in responding to his request to bring CIP 002-4 to the industry for balloting in 2010. He noted it has proved useful in discussions with Congressional staff and has had a positive impact on NERC's reputation and credibility in terms of standards development.

He wanted to clarify for the SDT what his thinking was on the path forward for the Team consistent with its SAR in addressing the FERC Order 706 directives. He suggested that it might be possible to address those directives in the CIP 10-11 framework the SDT has been developing or within the CIP 003-009 framework. He noted that many CEOs have expressed to him concerns about shifting away from CIP 003-009 and the documentation necessary for compliance, but stated that it is up to the Team under the standards development process to bring the proposal to the industry for comment and balloting.

He reviewed his comments to CIPC the past week which he characterized as exploratory in terms of consideration of a more coordinated and comprehensive approach to the goal of security of the BES among efforts such as the the CIP standards, the NIST smart grid initiative etc.. He noted he is considering possible approaches including putting together a team that might be in partnership with NIST to address this broader concept and that might lead to a comprehensive set or suite of voluntary "good practice" security guidelines over several years of work.

SDT Questions and Answers with Gerry Cauley

- The SDT is working under its SAR with directions to address FERC Order 706 directives. Is this still our charter?
- A: Yes, the SDT needs to address directives and chose which path or framework, in consultation with the industry, is best for reliability and industry implementation.
- The Team's concern is that every six months, we have had to change horses distracting us from addressing the core issues in FERC Order 706. Can you do anything to help us complete our task?
- A: That is consistent with my comments. Getting CIP-002-4 is a first step along the path and NERC will continue to support your efforts as a team.
- What will the collaboration with other areas of security look like?
- A: This is still in early discussions. It might involve forming a team to include industry, NIST, DOE, DHS and others under the NIST umbrella. The current CIP effort should continue and this is a longer-term prospect that will not conflict with the CIP effort. This possible set of guidelines might cover the entire electric system but would not supersede the CIP.
- The SDT has considered and tried to include aspects of the NIST approach. If the guidelines can bolster our effort, will they create the basis for a standard that has more credibility across the cyber security industry?
- A: Yes, both more credibility and acceptance. Your focus though presumes bulk power and the need to develop enforceable standards. I am suggesting a broader set of robust guidelines not limited to bulk power and enforceable standards.
- The SDT team has been frustrated by the limitations on standards writing in our efforts to address cyber security. Perhaps a more comprehensive set of guidelines would help industry.
- We need to ask if in five years whether we will have a more secure electric system? How will we get there? Our standards approach may be too narrow and leave industry exposed.
- How will a non-mandatory guidelines approach connect with 706 Order and compliance/audit system? Will the guidelines be subject to NERC audits?
- A: Nothing is enforceable under 215 unless it has gone through NERC standards process and approved by industry ballot and the BOT.
- The guideline may not be mandatory, but once written will it become industry practice and quasi-mandatory as best practice?

- A: This is a clear concern and a good point. We would rather have guidelines for good protection and address the audit/compliance fear through discussion with industry and improvements of our audit practice.
- Would NERC consider a certification model? There is concern about vendors implementing standards into products. There could be consideration of formal systems within the industry in parallel with the guidelines?
- A: Guidelines may help with the expectation of the industry to the vendors. There could be possible work with national labs on setting benchmarks for the vendors – exploring possibility of doing some testing through national labs to be sure vendors are meeting the expectations. This would be a separate initiative to investigate capabilities of the national lab – want vendors involved in developing the guidelines, then set up a testing system to ensure they are meeting the industry needs.
- We have fifty- plus directives in the order yet to be addressed in another version that will be out for industry review in the face of the implementation schedule for 002-4, assuming it is passed by the industry. Have you considered how all this will come together and address industry concern about changing landscape every year?
- A: For the foreseeable future we have to finish the SDT's efforts to address the FERC 706 directives. This other effort is more long-term with the hope that over a few years we can develop consensus on a voluntary tool kit that will not replace the standards. We will have to wait on experience in developing the guidelines before moving towards any corresponding standards development.
- There is a concern that once CIP 002-4 is approved by industry, FERC may direct us to answer additional questions. There is also a concern or perception that the industry may be more concerned about documenting compliance ("proper documentation") than in establishing better security. What happens if FERC remands 002-4?
- A: A dialogue with FERC would be a better approach as we have common purposes. Recent FERC orders have been clearer about their concerns with our standards and what we need to address, but we cannot rule out further questions about compliance. NERC hopes it will not be remanded, as it is far superior to the current standard.
- A NIST representative recently talked to an industry group about a new effort at collaboration – is this the same effort or different?
- A: Sounds possibly like the same concept.

The Chair thanked Gerry Cauley and he thanked the Team again for its hard work. The Chair asked members to reflect on this overnight and the Team can discuss further as needed on Wednesday.

On Wednesday afternoon the SDT discussed of Gerry Cauley's comments in relation to future CIP framework for the Team. The comments focused on completing the Version 5 work and clarifying the nature of the parallel process Mr. Cauley outlined. Below is a summary of the SDT comments:

SDT Version 5 Work and NERC Assistance

- The SDT needs to focus on and finish the Order 706 effort.
- The SDT believes that addressing the 706 directives will produce so many changes that if CIP 003-009 numbering were retained, that could be the only common feature remaining between the current CIP and Version 5.
- There is a lack of clarity on how the SDT could check with the industry other than developing the Version 5 and putting it out for comment and balloting.

- NERC needs to engage in a significant and serious marketing effort to rally the industry to whatever approach the SDT takes.
- The other issue is how to complete our work – apply appropriate and correct controls, no matter what we call it in terms of format. Now when we delete a requirement, it changes all the following numbers and that has been very confusing too.
  It is likely that after our 706 work, the only thing that will be left is the title. We are also trying to put in new items and address new issues. Simply putting new issues into a new 10 will confuse industry who now thinks 10 is a new High-Medium-Low strategy.
- We have the opportunity of announcing CIP 002-4's adoption by providing info on that and explaining the SDT's approach to the remainder with justification for the decision and the fact there will be heavy revisions to the current CIP. NERC should use this opportunity to begin preparing the industry for the SDT's release in the summer of 2011.
- Perception is everything, and we have a perceived problem with EEI who wants to stay with CIP 003-009. Members in the past have indicated the format is less critical than getting the substance correct.
- We are and will continue getting questions about what we are doing. We all, including NERC, need to help educate the industry.
- NERC should clarify the political support this group needs to get its job done.
- We have a NERC plan for communication which we should refine and send to him.

Potential Parallel Best Practice Initiative

- There is a need beyond the Team for NERC and FERC to review the proposed parallel effort;
- There are many excellent "best practice" guides that already exist in cyber security area that should not be reproduced through this effort.
- This needs further work and is presently confusing the industry and could district the SDT from its effort to complete the 706 work.
- Distinguish between national security concerns and standards development which has financial penalties attached;
- Gerry Cauley proposed two things in this parallel effort and we need to keep them separate. One addresses guidance and recommendations from retail metering to transmission. The other deals with how to secure it given perceived threat and vulnerabilities which NIST has done a good job of characterizing. The reality is that
  much of the good guidelines out there can be misapplied in the real world. The key question of what is right for our environment.
- The good news is that the puzzle is bigger than how NERC has approached this through standards. We need to move forward with producing the nitty-gritty cyber security standards. Focus on the detail work without worrying about the container. NSA and DHS have an agreement and there are several bills floating around Congress. The smart grid is being developed and the practical part is about to hit us on the head. We need broader thinking because of the financial realities – write good access controls and other baseline stuff. CIP 002-4 gave Congress perception of a broader scope. We need to get various parties talking to each other about the broader concept, while the SDT figures out what the requirements need to be.
- At recent conference a NIST representative suggested a new working group (not formed yet) will be looking for opportunities for coordination across standards for smart grid and its relationship to CIP standards. This should not change what we do – as far as CIP standards. We should not minimize the changes in the organization of the standards on the industry.

Companies now have multiple version folders trying to figure out what applies to what and when.
- For the last month and a half, there have been discussions about coordination between NIST and NERC. There is a shared interest by all parties in producing a more coordinated effort. They are looking at pretty much everything on the grid and the interactions needed to minimize inconsistencies. A working group may be formed at a December 15 meeting at NIST.
- Standards we are working on are trying to bolt security onto existing model. That may be different from the direction smart grid is working on. We are working with existing system focusing on reliability and there is the potential for big gaps between the approaches – FERC is most concerned about confidentiality – we need to understand their direction.
- For each interface NISTR defines what is the most important aspect and addresses from that perspective. There may be more in common than expected.

D. Related Cyber Security Initiative Update- CIP 005-4 Urgent Action

Scott Mix provided an update on the recent ballot for updates to CIP-005-4 regarding remote access. The ballot concluded with an 84.46% quorum, but a 42.89% approval rating. Approximately 100 pages of comments were filed from both the comment period and the ballot process. The team will be meeting to start responding to comments and modifying the requirement in response to comments.

Mr. Mix is also looking into whether a Compliance Application Notice (CAN) can be written to address some of the "double jeopardy" issues identified in the comments (i.e., indicating that some "global" requirements in existing standards will need to be applied to remote access if they are not already).

The desire is for the revised standard to be passed by industry and be submitted to FERC in time for the commission to act concomitantly with the CIP-002-4 action. Failing that, the guidance document developed for the standards revision will be handed over to NERC staff for posting as a document in support of the FOUO VPN Alert, and the standard requirement and industry comments will be turned over to the 706 team for its deliberation and consideration in the future version of the CIP standards.

Member Questions
- Will we file a CIP 005-4 in our next posting?
- A: Yes that had been the plan to include the conforming changes and request FERC to act on both petitions in the same order.

E. Related Cyber Security Initiative Update- CAN 005 Remote Access

Scott Mix noted that this has been noticed as withdrawn and would be undergoing revisions and then reposted.

Member Questions and Comments
- Mike Moon has indicated that the errors in the CAN needed to be fixed and that it is being withdrawn for redrafting.
- Heard several utilities are engaging lawyers to challenge the CAN.
- CIP 004 R4.2 CAN- problems noted include: it goes beyond the scope of requirement in CAN; revocation of access of secondary access systems- must be included in the revocation of access plan. Auditors audit to requirements and use the CANs in the audit.

II. REVIEW OF CIP-002-4 INDUSTRY COMMENTS AND SDT RESPONSES

Howard Gugel reported that the successive ballot of the Cyber Security 706 CIP Version 4 standards was conducted from December 1-10, 2010 and achieved a quorum of 86.83% and a weighted segment approval of 77.04%. Howard provided information on the difference between a successive vs. a recirculation ballot.

During the course of the three-day meeting, the SDT reviewed each industry comment and considered and refined strawman responses and agreed on final responses and on any changes to the standard documents. Each response was either unanimously agreed to by the SDT or the level of consensus was tested with the use of straw polling that helped direct refinements that built sufficient consensus (i.e. support of at least a 2/3's of the SDT members). Below are the key straw polls that lead to refined responses.

On Thursday morning, the SDT, following input from NERC Counsel, the SDT moved *(Tom Stevenson with Doug Johnson as 2nd)* to accept the proposed nuclear language with the motion carrying unanimously. Following that, the SDT moved *(Sharon Edwards with Bill Winters as a 2nd)* to approve the package of CIP 002-4 documents (including, Cyber Security — Critical Cyber Asset Identification CIP 002-4, Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4, CIP-002-4 Rational and Implementation Reference Document, Consideration of Comments on Successive Ballot for Cyber Security 706 – CIP Version 4 Standards, and Consideration of Comments on Project 2008-06). The motion passed 17 - 0 with 1 abstention.

III. REVIEW OF THE VERSION 5 FRAMEWORK

A. Framework Discussion and Review

Phil Huff reviewed the work of the Framework Team since the SDT meeting in Chicago in August. Since the Baltimore meeting the Team has developed a strawman meeting schedule, a style guide, and a communication plan. In terms of the overall schedule, Mr. Huff noted that the SDT will begin next month with a possible posting late June or in July. The Framework Team believes that continuing with a sub-team approach may not be the most effective way forwards. Instead they are recommending drafting assignments to Team members and utilizing the full team monthly meetings to review and refine strawman drafts.

The Framework Team has developed a "Style Guide" for drafting results based standards. It is recommending for the Team's consideration a BES cyber system identification using two impact levels: A (high) and B (medium) with a baseline level for low. Part of the communication plan that NERC will work with the Team to implement will include a change document that provides rationales for the proposed changes and mapping back to the existing CIP structure. Where possible the existing structure will be retained and justification will be provided for changes are needed. The following are the SDT comments seeking to clarify aspects of the Framework Team's proposal.

Clarifying Format and Organization

- Still remains to be seen what the whole package with explanatory boxes looks like as a package for filing – don't get hung up on the boxes or depend on them at this point for a final standard.

- Vegetation management is leading the charge on results based standards and establishing the format model
- Without assurance on how to use them, then they may be meaningless
- The idea is to establish a common style guideline the SDT can still use to consistently draft the requirements.

Clarifying Proposed CIP 11 "Organization Requirements

- CIP 11 are proposed as organization requirements that are not asset specific
- Everyone has to have a program. CIP 12 would look at asset impact levels of A, B and baseline – moving to a naming convention with critical assets in A, organizational in B and baseline everything else.
- Organization controls or include technical controls too in B?
- Organization controls but may need to adapt as we create. Everyone should review logs, but should access control be done on everything? This is a big issue for industry
- What about changing password? This gets into how we set and audit measures/
- The SDT will need help from enforcement to set language that is clear to both auditor and audited industry alike.
- The term "organizational" is used differently in CIP and industry depending on context.
- This proposal retains BES cyber system concept. Are we keeping critical cyber assets as a term? Are we pulling the term back?
- The idea is to make 11 level "agnostic." The bullets listed are related to the assets involved. Here you establish you must have a training program, then put details of what is required in the program in 12? Possibly.
- The list of examples here is illustrative not comprehensive. The examples here are organizational not baseline.
- Touch one system and you have touched a thousand more. The cost could be exponential for audit purposes. Keep in mind the distinction between organizational and baseline.
- The intent was organizational – across your organization, not asset specific – from audit standpoint what is the construct?
- Be sure the level of control is tied to type of asset
- Organizational focus replaces the old CIP 11 and there is no low.

Clarifying How Many Levels of Impact

- CIP 10 will identify the levels of impact
- Do we start from baseline and work up to high?
- We will have high and other? Everyone has to do the base or other even if they do not have CA's or CCA's – the high is divided into A and B as to what is required
- CIP 12+ is the devil in the details
- CIP 11 would apply to every entity
- Confused by levels A and B, and baseline. Should we have just high and other?
- Blending levels here? Organizational is not a level, it is all registered entities? Then have three impact levels of A, B and no impact with no regulatory requirement on the no impact level.
- Organizational requirements? Include controls to devices or just requirements for the organization.
- Does not suggest applying organization requirements to devices.

- Two threshold levels: high impact and those that impact reliability but are not critical assets. With a no impact level too.
- Identify every system or just A's and B's? Makes a difference for the scope of this effort.
- We need to establish a SDT consensus on levels and foundation before moving on without a common agreement.
- Level B system description – thought B was everything else that might impact A
- Need common understanding of what each level means
- As we draft controls – B is all the non-critical but some things may still need some controls.
- May help to look at specific examples. E.g. load shedding – we chose 300 mw, but in a low frequency event the end result may be it travels further than it should have and grows as it gets further from the event meaning more impact than it should have had from a cyber perspective.
- Still confused on the number of impact levels for systems? Are there three or two?
- It appears that baseline organizational requirements, may include some A's and some B's.
- This sounds like a compliance rather than a reliability concern.
- May need some baseline of control on all BES cyber systems with two levels of A (critical) and B (non-critical but connected) in terms of registered entities
- The team discussed the path of programmatic controls across programs without tying to assets. The reality is we are writing regulations, not guidance, with violations having penalties associated with them because of audits based compliance system.
- The team is thinking 2 versus 3 levels given our previous experience in trying to set medium level which was artificial. - in our business everything falls into a high that affects a lot of the BES and low that doesn't – level A is the critical or high, B is everything else in the organization.

Clarifying the Scope

- BES systems and non-BES systems – the latter not essential to running BES but the non-BES may be the avenue to attack the BES system.
- FERC does not have jurisdiction over the non-BES system such as email systems.
- CIP 10 is similar to 002-4 – anyone feel there is a need for distinction of non-BES system – favor two levels versus three levels? Just considering impact levels, not connectivity here.
- Working through three levels proved problematic – organizational level for everything and the more for high level – two level system
- We have to work off of a definition of BES system – that is the purview or scope of our work.
- What is the population of system in the scope? Those that impact the reliability of the BES system are the target, not every non-BES system.
- Connectivity determined level, but if not in the inventory of assets how do we ensure it is protected?
- Cyber system is not easily defined. It would be unfair to say it has to be defined to a common understanding. The industry will need flexibility (as cyber systems don't look alike in terms of age and functions) and security boundary is the foundation issue.
- If connected to BES cyber system then it becomes a BES cyber system component though it is not a cyber asset and it needs protection.
- It crosses a threshold that requires you to apply controls and makes it a component once connected
- That is the point in BES cyber system maintenance section in the old CIP 11.

- BES cyber systems have protections – outside cyber system there are components that need protection because they are attached to the system for purposes of maintenance but are not part of the system but a component for maintaining the system
- How are controls on system and controls on components on the system different?
- We can distinguish physical access to component but not the non-physical access.
- May have to break up into more granular level to assign appropriate protections.
- Most of the requirements are written for the cyber level – do we need a different term than "component" or at least for the ancillary ones that get plugged into the system
- Are we dealing with the physical location or type of equipment? The former may differ depending on location but the latter will not.
- Measures – the format is table with first column of requirements and next column with measures – bullets are the guidance for writing measures.
- Based on our discussion as far back as January 2010 (Tucker) we focused on what is the primary intent of the attack.
- Ultimately goes back to 10
- We assume in 002-4 that identified assets are targets in themselves as A and B's are either targets in combination with or avenues of attack to A's.
- Is it a BES cyber system if not connected to anything else – multisite attack?
- In 002-4 we based bright line on impact to BES of its loss so that A is based on impact to BES, B is combined impacts to BES, and others have no impact on BES
- We identified the high impact and those that support the high level. The rest should shake out to those in the BES system that require organizational control will be too difficult to test out all the lows in combination that may impact BES. It may be the right thing to do and appropriate, even if hard to audit. We have to allow entities the flexibility to determine. Already protecting systems to protect our assets, not just to comply with audits – mandatory compliance controls for high assets, limited controls on low and let companies figure out the middle

Independent Certification Process

- Should the SDT consider the option of standing up an independent certification body to establish what qualifies? If it doesn't fit within the SAR and scope of this SDT should we approach NERC about expanding scope to consider certification process?

B. Results Based Standards Training

In preparation for the Version 5 drafting challenges, the SDT engaged in a results based standards review and training conducted by Keith Heidrich FRCC, on Thursday of the meeting. Mr. Heidrich has participated on an ad hoc NERC team convened by Gerry Cauley which has been developing the concept of a results based standards approach.

He outlined the training objectives as:

- Identify and give examples of the elements that define a results-based standard
- Analyze the current standards and requirements for weaknesses
- Identify the needs, goals, and objectives for this
- Create an initial draft of this standard and requirements using result-based methods
- Create measures and necessary supporting material for the standard and requirements

The training covered: Results-based standards/requirements – what are they and why they matter; Scope–what you need to know before writing requirements; Standard requirements – observations and improvements; and Where information is recorded – templates.

Mr. Heidrich noted in a results based approach, the SDT needs to answer the question: *Who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome?* A Standard is a portfolio of requirements designed to achieve an overall defense-in-depth strategy and comply with the quality objectives with each requirement having a role in preventing system failures. Requirements within a standard should be complementary and reinforcing. He distinguished among performance based, risk based and competency based standards.

SDT Member Questions and Comments

- Is cost an appropriate or allowed consideration? A: Yes, but not as a driver – it is an issue in almost any TFE – it is "a consideration for smaller entities but not at consequence of less than excellence in operating system reliability"
- Do we have to establish caveats as to size or cost effectiveness? FERC Order 706 asked industry to establish reasonable and appropriate measures – reliability impact is a safer argument to make for smaller entities – but if everything is connected then smaller entity can impact the BES reliability. A: The CIP 005 team struggled with this issue too and came up with a range of solutions including less costly approaches to minimum levels of protection – can't compromise requirement for cost reasons but you can carve out subsets of applicability based on impact to the BES that cover smaller entities. This is difficult to do if entities are interconnected.

C. Next Steps for Developing the Framework

On Thursday, Phil Huff noted that based on the review and discussion at this meeting the Framework team would be proposing two impact levels with all other being those items falling outside BES system definition. The Team will present a refined proposal in January taking the SDT input into consideration. For those in those covered in one of these two levels there will be multiple types of controls to be applied. It will get down to the drafting requirements in a consistent format. We recognize detail still needs to be worked out.

Member Comments

- Just because we changed labels doesn't make it easier to fix the problems.
- Do NERC standards development requirements allow blank requirements? No
- We need to retain flexibility to make course correction if industry pushes back. We will still need controls regardless of the structure – spend time wisely developing controls then put into structure at the end.
- We need to get on with technical work and worry about style and format later.
- Agree we need to move forward to writing the requirements – guidance to date allows us to use a format to capture and write the controls.
- The Access Control sub-team continued to work and the SDT could use their work as a strawman to test as an example. The sub-team worked with three levels but struggled with

- "medium." Their work as our example may help understand how the propose "two level" system would work

The Chair and Vice Chair noted that the expectation is that following the January 2011 session the Framework Team would dissolve and an open set of SDT meetings will be used to refine the proposed framework through review of strawman drafts of requirements. The Framework Team will set up conference calls in January in advance of the Columbus meeting.

IV. NEXT STEPS AND ASSIGNMENTS

The Team reviewed the steps and assignments leading up to the Columbus meeting. The Framework Team will be meeting in early January 2011 to prepare documents for the SDT to review at the January 2011 meeting. The recirculation Ballot is expected to close on Friday, December 31 COB. NERC staff will notify the SDT of the ballot results.

The Chair thanked Rich Kinas and the OAS for the hosting of the SDT in Orlando.

The meeting adjourned at 4:40 on Thursday, December 16, 2010

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 29th Meeting Agenda
December 14, 2010, Tuesday- 8:00 AM to 6:00 PM EST
December 15, 2010 Wednesday- 8:00 AM to 6:00 PM EST
December 16, 2010 Thursday- 8:00 AM to 6:00 PM EST
Orlando Utilities Commission Offices
6113 Pershing Avenue
Orlando FL

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 results of the 2nd Ballot and test consensus on responses to industry comments on CIP 002-4 and, if needed, on any changes for inclusion in a CIP 002-4 3rd ballot.
- To review, refine and test support for recommendations of the CIP Version 5 Framework Team.
- To participate in a Results Based Standards Development Training
- To agree on next steps and assignments

Tuesday, December 14, 2010 8:00 a.m. - 6:00 p.m. EST
- Introduction, welcome -*(Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review results of 2nd Ballot CIP-002-4*(Morning)*
- Draft responses to industry and consider any changes to CIP-002-4 *(Morning & Afternoon)*

Wednesday, December 15, 2010 8:00 a.m. - 6:00 p.m. EST
- Seek Motion to Adopt SDT Responses to Industry, and if needed, any changes for inclusion in the 3rd Ballot. *(Morning)*
- Overview of Results Based Standards Development and CIP Version 5- Howard Gugel NERC *(Morning)*
- Receive a Version 5 Framework report *(Morning)*
- Review Draft Strawman Documents and discuss key issues *(Afternoon)*
- Review and initial testing of the acceptability of the approach as refined *(Afternoon)*

Thursday, December 16, 2010, 8:00 a.m. - 6:00 p.m. EST
- Results Based Standards Training- Keith Heidrich, FRCC & Howard Gugel, NERC *(Morning & Afternoon)*
- Review Version 5 Framework in light of Results Based Approach
- Test SDT Support for the Version 5 Framework *(Afternoon)*
- Review Work plan for the Version 5 Framework *(Afternoon)*
- Review SDT January, 2011 Columbus Meeting Agenda (*Late Afternoon)*

Appendix # 2 Attendees List
December 14-16, 2010 Orlando

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. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9.Rich Kinas	Orlando Utilities Commission
10. John Lim, Chair	Consolidated Edison Co. NY
11. David Norton	Entergy
12. David S. Revill	Georgia Transmission Corporation
13. Tom Stevenson	Constellation
14. Keith Stouffer	National Institute of Standards & Technology
15. John Van Boxtel	WECC
16. William Winters	Arizona Public Service, Inc.

SDT Members Attending via ReadyTalk and Phone

17. Jackie Collett	Manitoba Hydro
18. William Gross	Nuclear Energy Institute
19. Scott Rosenberger	Luminant Energy
20. Kevin Sherlin	Sacramento Municipal Utility District
21. John D. Varnell	Technology Director, Tenaska Power Services Co.
Gerry Cauley	*NERC (Tu)*
Scott Mix	*NERC*
Howard Gugel	*NERC*
Ralph Anderson	*NERC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Not Participating

Jeff Hoffman	U.S. Bureau of Reclamation, Denver
Patricio Leon	Southern California Edison

Jonathan Stanford	Bonneville Power Administration
Bradley Yeates	South Nuclear Operating Company

Others Attending in Person

Robert Preston Lloyd	Southern California Edison
Jim Fletcher	American Electric Power
Jason Marshall	Midwest ISO
Roger Fradenburgh	N&ST
Brian Newell	American Electric Power
Guy Zito	NPCC
Rob Wotherspoon	OUC
Mike Keane	FERC
Kevin Ryan	FERC (Tu/W)
Mark Simon	Encari

Others Attending via Readytalk and Phone

December 14
Matthew Adeleke, Vincent Le, Lawson, Rob Gross, William Bussman, John Hofstetter, Tom Kelly, Justin Doetzl, Joe Artz, Kevin Kittey, Drew Lopez, Andres Camm, Larry Wilson, Bryn Powell, Maggy Hasha, Christine Bargen, Jan Hardiman, Rod Hoffman

December 15
Scott Hoffman, Jeff Powell, Jim Bussman, Nathan Mitchell, NathanRyan, Kevin Sherlin, Kevin Le, vincent Antonishen, Rob bargen, jan Wilson, Bryn adeleke, matthew Barry Barry Lawson, Drew Kittey, Drew Hasha, Christine Rod Hardiman, Andres Lopez

December 16
Drew Kittey, Maggy Powell, Rod Hardiman, John Bussman, , Vincent Le, Bryn Wilson, Andres Lopez, Jan Bargen, Brian Newell, Barry Lawson

Appendix #3 NERC Antitrust Compliance Guidelines

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

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

Final SDT CIP 002-4 Documents

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

Appendix #5 SDT Sub-Teams

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese, Bill Winters *(Observer Participants: Roger Fradenburgh, Robert Preston Lloyd)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
CIP 002-4 Drafting Team	John Lim (Lead), Jim Brenton, Jackie Collett, Jay Cribb, Sharon Edwards, Doug Johnson, Rich Kinas, Dave Norton, Dave Revill, and Bill Winters *(Observer Participants: Rod Hardiman; Jim Fletcher; Bryn Wilson)* *(FERC: Mike Keane, Peter Kuebeck; NERC: Scott Mix)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*
Framework CIP 010 &011	Dave Norton (Lead), Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. *(FERC: Mike Keane; NERC: Scott Mix)*