NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes

Cyber Security Order 706 SDT — Project 2008-06

May 11, 2010, Tuesday | 1–5 p.m. CDT
May 12, 2010, Wednesday | 8 a.m.–5 p.m. CDT
May 13, 2010, Thursday | 8 a.m.–noon CDT
Dallas, Texas

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 May 11–13, 2010 Meeting Summary Contents

EXECUTIVE SUMMARY

On Tuesday afternoon (May 11, 2010), the SDT Chair, John Lim welcomed members and other participants to the SDT's 22nd meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines. The host Scott Rosenberger, a SDT member, welcomed everyone to the facilities and covered logistics. Bob Jones, facilitator, reviewed the proposed meeting agenda. On Thursday morning the SDT approved without objection the meeting summary for the April 13–16, 2010 SDT session in Atlanta, Georgia.

Bob Jones reviewed with the team the process followed to produce and adopt the draft CIP standards for posting to the industry for informal comments. The team discussed what worked and what could be improved going forward.

Stuart Langton reviewed the SDT work-plan noting that the team has been meeting every deadline on time. He suggested the team should have confidence in the work done and that we will strive to continue this level of performance as we go through the rest of the year. He noted that last week was a big milestone with the unanimous adoption of the draft CIP-010 and CIP-011 standards for posting to the industry. Next week, the team will host a technical workshop for the industry stakeholders in Dallas, TX. The SDT is looking to receive the industry's initial feedback and a sense of their assessment of the current draft standards at this workshop.

On May 27, the SDT will be meeting with FERC staff in Washington D.C. to present the draft CIP standards and seek their initial feedback on the approach and the acceptability of the text.

The input received from the industry stakeholders through the technical workshop will be integrated with the industry comments received by June 3, 2010, in response to the informal posting of the draft CIP standards. The comments will be distributed to the SDT members, the sub-teams by close of business on June 4, 2010. The SDT members will be asked to read each of the comments before the meeting in Sacramento (June 8–11).

The December 2009 posting of CIP-002-4 resulted in NERC receiving about 500 pages of industry comments for 3 CIP standard requirements. With the current 30+ requirements included in the drafts of CIP-010 and CIP-011 submitted for informal posting, there will likely be a significant volume of comments and pages to read, digest, and consider. Since the current posting is part of an informal comment process, the SDT is not required to respond to each individual comment received. A "consideration of comments" summary document will be produced by the SDT to group and highlight the major comments and issues received as part of the industry feedback. This summary document will be posted prior to the first formal comment period, which is scheduled to begin in July 2010.

The Sacramento meeting will be an important one for the SDT in terms of responding to industry suggestions and comments and refining CIP-010 and CIP-011 for posting later in July. Following the July meeting in Pittsburgh, the team is scheduled to meet in August in Chicago, September in Winnipeg, October in Toronto, November in Baltimore, and December in Tampa. The

schedule shows three possible ballots with the possibility of revising the standards based on the responses received for each ballot.

The Chair noted that NERC Chief Security Officer, Mike Assante, has announced he is leaving NERC. NERC has posted a job notice to the industry. Keith Stouffer provided an update on NIST smart grid activities. Dave Norton noted there was recovery ARA funding for smart grid development of more than $3 billion, and DOE is requiring "cyber security plans" from applicants to receive and/or retain funding.

The team discussed the development of the documents for the April 2010 informal comment posting, noting that the positive experience by the SDT has resulted in an effective small group process that can efficiently produce the necessary documents. It was agreed that there needed to be better coordination when the sub-teams are working in June and July to produce the draft CIP standard documents for posting. The SDT discussed the industry comment process and possible scenarios, including industry push back. Some noted that the work over the next few months to coordinate all of the activities including the incorporation of industry comments will present a leadership and practical challenge for the SDT and its members. As one member put it, "What is needed now is a focused motivational and leadership effort at NERC to get behind what we've done. If we show division on the team, the industry will not be supportive of our work."

Stuart Langton provided an overview of the draft changes in the SDT consensus procedures adopted in November 2008. On Thursday morning, the SDT reviewed the draft changes to the consensus procedures and engaged in discussions concerning quorums and electronic voting, but was unable to decide on the wording changes. Stu Langton proposed and the Chair agreed to ask Bill Winters and Jon Van Boxtel to serve as a drafting sub-team to review the SDT discussion and come to the June meeting with suggested revisions for adoption by the SDT. Mr. Winters and Mr. Van Boxtel agreed.

On Tuesday, the Chair noted that the Technical Workshop for the industry scheduled for the following week in Dallas, had approximately 240 industry persons who have registered, with no more than two per company, to attend in person and many more registering to join on the ReadyTalk web-conference. The SDT agreed to conduct a Tuesday afternoon walk-through of the presentations from 2–5 p.m. with Gerry Adamski, NERC Vice President and Director of Standards. Since NERC was not going to produce hardcopy workbooks for the workshop attendees, the SDT needed to complete the presentation materials so they could be posted prior to the workshop. As part of the workshop announcement, NERC requested the industry submit questions ahead of time. The plan is to sort the written questions submitted by the industry along with the questions submitted by the audience during each session so that they could be answered by the respective SDT sub-team members.

After discussion, the SDT agreed to ask workshop participants to utilize session comment forms they will receive when they sign in to offer specific questions and suggested changes in the draft text of the standards. All of this would be captured and posted in a workshop summary document that will be part of the informal comment record. The SDT discussed how to handle questions about topical areas upon which the team had not reached agreement and on questions that the SDT did not have clear, concise answers.

Gerry Adamski joined the team on Thursday by phone to discuss the workshop approach and his role. He committed to crafting a set of talking points that he will share with John Lim and Phil Huff to make sure all are on point and provide a consistent set of expectations for the workshop. Scott Mix noted he would present high-level concept ideas for feedback regarding the implementation plan with help from a SDT drafting group.

During the final review of the draft CIP-010 and CIP-011 standards in late April, the SDT identified a number of issues that needed attention as the team went forward with refining the draft. These were presented and discussed by the team on Tuesday afternoon and included:

- Review the clarity of item 1.1, Attachment 2 – Generation Facilities and criteria for Contingency Reserve and Reserve Sharing;
- Review the appropriateness for delegations to be made by the Senior Manager for any exceptions (CIP-011 R2 & R3);
- Review of User-type access (R3)
- Review the need for network device training (Operators, etc.) (3.2)
- Combine tables for electronic and physical access control systems (R6, R20, & R22)
- What do the blank cells mean in the tables in instances where a timeframe is given? (R9)
- Monitoring the baseline configuration means monitoring the physical location as written. (R23)
- What timeframe to use for issuing alerts (Table entry 18.2)
- Need to address what disciplinary actions are? Should physical or cyber access be revoked?
- Combine the revocation of physical and electronic access requirements (including remote access) into one topical area of the standard

The SDT reviewed and discussed initial sub-team draft presentations on Wednesday morning and agreed on some basic formatting. A template had been circulated to the sub-team leads before the meeting which was modified in the initial review. For each of the following topics, slides were developed by the sub-team members and refined following two rounds of review and discussion with the full team:

1. Overview and Approach
2. CIP-010 (formerly CIP-002)
3. Personnel and Physical Security (CIP-011 R2–R6)
4. Electronic Access Control (R7–R14)
5. System Security (R15–R19) and Boundary Protection (R20–R22)
6. Configuration Change Management R23 Information Protection & Media Sanitization R24–R25 BES Cyber System Maintenance R26
7. Cyber Security Incident Response (R27–R29) BES Cyber System Recovery (R30–R32)

Each sub-team developed a table mapping the changes from Version 3 of the CIP standards to the current version. A document identifying the FERC directives and responses was also produced.

The team discussed the FERC Order 706 issues that will be addressed by the SDT in 2011 following adoption of the CIP-010 and CIP-011 standards. Scott Mix reviewed a table with the remaining FERC

directives. He characterized these as 'up the 12 issues that are large, controversial and complicated' (e.g., multi-procedural defense in depth and forensics, etc.). Scott Mix suggested that at the workshop the SDT should make it clear and obvious to the industry we have lopped off some big topics that will be addressed after finishing the current work.

The SDT discussed what kind of guidance documents the team should be producing for industry implementation. Some members noted the value of guidance documents to help the industry understand the requirements. On Thursday morning, Mark Engels, Chair of the CIPC Working Group Control System for Security joined the team and discussed their related work on developing consistency on when and how to draft of standards guidance documents. The Chair and Vice Chair noted that at the Sacramento meeting a Guidance drafting sub-team would be formed.

Scott Mix presented the implementation plan concepts and noted a SDT sub-team was formed in Atlanta to draft the plan.

On Thursday, the SDT discussed the upcoming FERC/NERC meeting on May 27 and proposed to schedule a preparation meeting of the SDT early in the week of May 24. Several SDT members indicated they were planning to be present for the session.

The SDT also discussed the Sacramento agenda and the likelihood of a very large volume of comments that will need to be read, reviewed, and decisions made on how to respond and whether to adjust the draft standards. It was agreed that after review of the questions and responses from the workshop (including the online comments) and review of the questions related to format of CIP-010 and CIP-011, the sub-teams should plan to meet Tuesday and Wednesday and report back to the full SDT on their recommendations.

It was agreed that after the Sacramento meeting there would be a need for weekly sub-team meetings and possibly sub-team leads meetings. The project schedule will need to be adjusted to reflect these new meetings, plus target SDT meetings to develop drafts of the standards for NERC staff to review in advance of the July meeting in Pittsburgh.

The Chair thanked Scott Rosenberger and Luminant, especially Linda Jojo, CIO of Energy Future Holdings for the excellent support and facilities provided to the SDT in hosting this meeting.

The meeting adjourned on Thursday at 12:30 p.m.

I. AGENDA REVIEW AND WORKPLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim and Vice Chair Phil Huff welcomed the members to the SDT's 22nd meeting that thanked them for their hard work under pressure to get the CIP-010 and CIP-011 version out on time in early May. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Scott Rosenberger, a SDT member, welcomed everyone to the Dallas, Texas Luminant meeting facilities and covered logistics and emergency procedures.

On Thursday morning, Linda Jojo, CIO of Energy Future Holdings (Luminant) offered brief remarks acknowledging the SDT's important but challenging work. She said that she knows the industry has a range of opinions on cyber security and that this is "an inflection point for the industry." She urged the yeam to focus on protecting what's important and but not going overboard. She thanked the Team for what it is doing on behalf of the industry.

The Chair reviewed the following meeting objectives:

- Review the work plan and schedule;
- Review and adopt the 2010 Consensus Procedures as refined;
- Receive updates on other related cyber security initiatives;
- Receive a NERC overview of the Technical Workshop;
- Review and Refine "Parking Lot" Issues from the April, 2010 CIP Documents for Informal Posting;
- Sub-teams will: detail how FERC directives have been addressed; develop a "change documentation" draft; develop Technical Workshop Presentations; and identify possible guidance areas and bullet lists of guidance content;
- To review a proposal for drafting a CIP Guidance Document for posting in July, 2010;
- To review how the SDT will develop the CIP Measures, VSLs, and VRFs for posting in July, 2010;
- To review the May 27, 2010 meeting with NERC/SDT and FERC; and
- Agree on next steps and assignments

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

Bob Jones, facilitator, reviewed the proposed timed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the April 13–16, 2010 SDT session in Atlanta, Georgia.

B. Work-plan Schedule Review

Stuart Langton reviewed the SDT Work-plan noting that the team has been meeting every deadline on time. He suggested the team should have confidence in the work done and that we will strive to continue this level of performance as we go through the rest of the year. He noted that last week was a big milestone with the unanimous adoption of the draft CIP-010 and CIP-011 standards for posting to the industry. Next week, the team will host a technical workshop for the industry stakeholders in Dallas. The SDT is looking to receive the industry's initial feedback and a sense of their assessment of the current draft standards at this workshop.

On May 27, the SDT will be meeting with FERC staff in Washington, D.C. to present the draft CIP standards and seek their initial feedback on the approach and the acceptability of the text.

The workshop industry input will be added to the FERC staff comments and online comments received by Thursday, June 3, 2010 and distributed to the SDT members and the sub-teams by the weekend prior to the Sacramento meeting. The members were asked to read each of the comments in advance of the meeting in Sacramento.

The December 2009 posting of CIP-002-4 resulted in NERC receiving about 500 pages of industry comments for 3 CIP standard requirements. With the current 30+ requirements included in the drafts of CIP-010 and CIP-011 submitted for informal posting, there will likely be a significant volume of comments and pages for the SDT to read, digest, and consider. Mr. Langton noted that since the current posting is part of an informal comment process, the SDT is not required to respond to each individual comment received. The plan is to prepare a "consideration of comments" summary document that will group and highlight the major comments and issues received as part of the industry feedback. This summary document will be posted prior to the first formal comment period, which is scheduled to begin in July 2010.

Mr. Langton noted that the Sacramento meeting will be an important one for the SDT in terms of responding to industry suggestions and comments and refining CIP-010 and CIP-011 for posting later in July. Following the July meeting Pittsburgh, the team is scheduled to meet in August in Chicago, September in Winnipeg, October in Toronto, November in Baltimore and December in Tampa. The schedule shows three possible ballots with the possibility of revising the standards based on the responses for each ballot.

SDT Discussion of the Schedule

- Scott Mix explained the modification for this approved by Standards committee which is similar to way ISA does it which allows the SDT to make technical changes and modifications to standards language between ballots. Not restricted to 2 ballot periods.
- The new NERC Procedures are currently being balloted (in recirculation).
- Positive features. Streamlining and being more responsive during the ballot period.
- Insertion of informal comment helpful.
- How we respond to informal comments will be very important because we will go to ballot before responding to the comments received after the July posting.

- In terms of industry comments received on June 3, is there a way to gather them together in "buckets" so the sub-teams can take the lead in reviewing the comments and considering possible changes in 010 and 011.
- Each member has to review every comment.
- We should reserve some of the time for sub-teams meetings and review of comments.
- There is a Webinar tentatively scheduled in August as part of the outreach.
- SDT and sub-teams need to plan on meeting the last two weeks in June and first week in July to prepare the documents for posting following the July 13-16 meeting in Pittsburgh

C. Related Cyber Security Updates

The Chair noted that NERC Chief Security Officer, Mike Assante, has announced he is leaving NERC. NERC has posted a job notice to the industry. Keith Stouffer provided an update on NIST smart grid activities. Dave Norton noted there was recovery ARA funding for smart grid development of more than $3 billion, and DOE is requiring "cyber security plans" from applicants to receive and/or retain funding.

SDT Comments

- The NIST Smart Grid group had been working on interface issues before, but now working on real standards.
- There was recovery ARA funding for smart grid development of more than $3 billion. DOE is requiring "cyber security plans" in order to receive and/or retain funding.
- About 7 members of the SDT are involved in drafting cyber security plans.
- The Aurora response is also keeping people busy.
- DOE road map to secure control system. Version 2- is about to come out. DOE Joint working group- intersection. Security R & D, Vendor subgroup, Roadmap subgroup (Perry Peterson and Tim Roxy).

II. REVIEWING THE SDT PROCESS

A. Team Debriefing of the Process for Developing the Draft for Posting

The team discussed the April 2010 development of the documents posted for informal comment noting that the experience demonstrated that the SDT has developed an effective small group process that can produce the documents. It was agreed that there needed to be better coordination when the Sub-teams are working in June and July to produce the draft CIP standard documents for posting. The SDT discussed the industry comment process and possible scenarios, including industry push back. Some noted that the work over the next few months to coordinate all of the activities including the incorporation of industry comments will present a leadership and practical challenge for the SDT and its members. As one member put it, "What is needed now is a focused motivational and leadership effort at NERC to get behind what we've done. If we show division on the team, the industry will not be supportive of our work."

What Worked	***What Can Be Improved***
Sub-team were able to complete their work	Enhanced coordination and communication
Sub-team leads coordinating calls	Better planning and advance scheduling

	of SDT and sub-team meetings
SDT work with NERC staff	Wasn't ready with product in Atlanta, need to be ready in Pittsburgh.

SDT Discussion of Industry Comment Process and Scenarios

- Do we need to do some planning to handle the scenario if the comments are something other than "tweak this" but resoundingly receive industry push back?
- Scenarios for adjusting
- Some members noted they were not getting good "vibes" from the industry
- Others noted positive comments received.
- Sent the draft 010 and 011 to the NIST Smart Grid to get comments and back.
- If we determine that we have more work than anticipated in light of the industry input, we will need to go back to the Standards committee to get the schedule adjusted. If there is work to be done but can't do it in the schedule due to the reaction of the industry. This is one of the NERC's top 10 projects and it will be difficult to slip on schedule. We will have to figure out how to get back on track.
- FERC's expectation is that NERC will have something filed by the end of 2010. Who goes to FERC with the bad news? NERC would have to convey this to FERC as part of an information filing.
- NERC needs to talk to companies to see what the maximum output of this team could be. We in effect met 2-3 weeks consecutively in April and May.
- Already stretching by 30%? Stretch any more its going pop.
- If we get back significant vitriol from the industry, may have to back into situation with a "tiger team."
- We are asking for feedback and the team needs to pitch this product positively at the workshop.
- The format and re-numbering standards should not produce shock in the industry.
- This is a long term- functional approach which is stronger and more robust. The industry won't pass if we are not positive about it.
- Note that it took 3 years to do Version 1 and that was added to the several years of development of UA 1200.
- Can't be enthusiastic about something I don't believe in. The wording and organization I don't agree.
- Experience- high order feedback. Compliance people, 1 standard. Whole industry will be out of compliance every year. Why did you have to reorganize everything?
- Mix of feedback. Quick draw on what are we doing and why. Have to try to provide the why. Industry wants that. They don't want to reject it outright. They want to understand the technical reason for these changes. What justification for re-shuffling the deck. Many have put in time and $$ to be compliant with the current version. If we don't have a good "why" we will have problem.
- Discussing comments- when we will have the response on the format.
- Disappointed the SDDT wasn't able to get the guidance ready to post with the draft 010 and 011. Not having the guidance and prepared statements for why we are doing it. People who got slapped in face, didn't know it was coming. It will be imperative that we do a good job explaining changes and why we've done this.

- This is at base leadership challenge. What is need now is a focused motivational and leadership effort to get behind what we've done. If we show division on the team, we the industry will not be supportive of this. We need Company executives to understand, coalesce and lead this effort.
- By the end, when we posted the documents for informal posting, none of us thought we have the final product. We will not be putting this on the pedestal. We are hoping to get industry assistance on improving it..
- Parking lot- tool from the team. Tool to get where the development team to build consensus. We do need to be enthusiastic.

B. Review of SDT Consensus Procedures

Stuart Langton provided an overview of draft changes in the SDT consensus procedures adopted in November 2008 procedures on Tuesday. (See, Appendix #5) The facilitators wanted to take a check on our procedures and see if they could be clarified where needed and improved before the SDT gets to its next milestone in July. There are several revisions including provisions for: electronic voting; clarifying the 2/3's quorum consistent with the NERC SDT rules of procedure (a version of the current adopted rule suggests 51%) and clarification of the use of Robert's Rules after facilitated review and consensus building. Mr. Langton encouraged members to approach the facilitators between now and Thursday with any suggestions or improvements that the Team could review.

On Thursday morning, the SDT reviewed the draft changes to the consensus procedures and engaged in a discussion raising the following points:

- Question about chair only calling for electronic vote. Should it also permit the Vice Chair?
- Use a motion to call for an electronic vote? Note, the provision applies when you can't place a motion on the floor because of lack of quorum.
- What about when you don't reach a 75% can you use it then? Not if there is no quorum.
- Clarification regarding quorum. It appears the November 2008 meeting summary text has the quorum being adopted at 2/3 but the consensus procedure included in the appendix of the meeting summary has it as 50%+.
- "Vote for posting for industry comment." Is this too narrow? How else would be able to go with less than the 75% if you were not asking the industry for input. This approach doesn't make sense in the SDT posting for ballot.
- Electronic mail vote language. Maybe add "Specified time frame." What is a reasonable expectation in terms of timing- 24 hours? How much detail does the procedure need?
- Note that the SDT's limited experience with electronic voting wasn't very successful.
- Don't have a problem with deadline. Perhaps "add reasonable" to the electronic voting provision.
- Do we need to outline a method for initially developing a quorum by email and then proceed with a vote?
- Email voting was not the issue was raised in Atlanta. Rather the question was when a quorum is present and members are involved in the discussion leading up to a vote on a proposition but have to leave the room before the vote.
- For example, Jim Brenton had been in the discussion, had to leave for a plane, tried to call in to participate but had to board the plane. He indicated a preference. On the other hand Frank Kim left the day before the discussion and verbally expressed a general preference to another member

but it wasn't counted when the vote took place the next day since it was expressed prior to the SDT discussion the following day.

- Is there a procedure we could adopt where a member participating in a discussion of an option could lodge a preference without it be viewed as a "proxy" which is not permitted under NERC's procedures.
- This would only work with the words being written down, discussed and considered and not changing after the member departs.
- In those circumstances, perhaps providing for a procedure to leave with the chair or vice chair a written statement of their preferences? Provided the voting is on same motion or is electronically provided later.
- In Atlanta we had a known quorum. Do we need to have a known state prior to electronic voting. How to transition from quorum to the vote?
- Scott Mix suggested that the Email comes with own quorum in that there will only be a decision if a quorum is reached and the vote is 75% or more.
- If someone leaves before wording is available, perhaps we could make an effort to contact person to get to it.
- Electronic voting- may be useful and serve other purposes for the SDT. For example when the SDT does an entire meeting electronically.
- SDT members continue to have the responsibility to show up in person for by readytalk.
- Look at electronic or other means.
- John Van Boxtel offered a motion to move forward with changes but to delete the proposed electronic voting language and come back with language for consideration by the SDT in June. There was not a 2nd on the motion. John Varnell offered to conditionally 2nd the motion with a "friendly" amendment to leave the electronic voting language in. This was not considered friendly by the maker of the motion.
- The Chair expressed concern that there may be undercurrent that somehow members have or might "game the SDT voting system" suggesting a lack of trust in the team?
- Not suggesting gaming is the issue, but don't want to adopt procedures that allow for manipulations of the team in the future. It should be the smart and proper thing to do now in advance of decision making.

Stu Langton proposed and the Chair agreed to ask Bill Winters and Jon Van Boxtel to serve as a drafting team to review the SDT discussion on the procedures and come back in June with some suggested revisions for review and adoption by the SDT. Mr. Winters and Van Boxtel agreed.

III. PREPARING FOR THE CIP 010 AND 011 TECHNICAL WORKSHOP

A. Technical Workshop Overview and Preparation

On Tuesday, the Chair noted the Technical Workshop is scheduled for next week in Dallas and there are 270 industry persons and SDT members registered, with no more than two per company, to attend in person and several hundred more on the ready talk and phone line. Scott Mix noted that as of Tuesday, NERC had not received any questions yet from industry to be reviewed at the Workshop. The SDT agreed to conduct a Tuesday afternoon run through with the SDT. 2-5 p.m with Gerry Adamski NERC

Director of Standards. Since NERC was not going to putting together workbooks the Team needed to complete the workshop presentation materials so they could be posted by Thursday.

NERC requested the Industry to submit questions ahead of time the plan was to go over written questions from the audience on cards for each session to be answered by SDT sub-team members. After discussion, the SDT agreed to ask Workshop participants to utilize session comment forms they will receive when they sign in (also available in electronic form from the NERC Workshop website). This will encourage participants to offer specific suggestions for changes in the draft. All of this would be captured and posted in a workshop summary document and will be part of the informal comment record.

The SDT discussed how to handle questions on areas the Team had not reached agreement and on questions which the SDT did not have answers. It was agreed that members will speak as individuals consistent the Team's broader statements and be candid about any differences that have emerged on the Team on issues such as format, etc. with the intent of flagging these areas as ones for industry feedback. Some suggested the best way to answer such questions may be a posing a question back asking how they believe the issue should be addressed. The general approach ought to be to encourage industry participants to provide constructive suggestions on how to fix issues and concerns they may have with the draft.

Gerry Adamski joined the Team on Thursday by phone to discuss the Workshop approach and his role. He noted the registration process is complete with over 270 people registered in person and over 400 registered for readytalk/phone. The Team related the idea of some informal face-to-face time during breaks and in the evening reception and providing session comment forms to as part of the agenda packet to be collected at the end of the workshop. There was SDT discussion of whether an objective of the Workshop is to measure of how much industry supports the concepts the SDT has developed so far. Some noted that it needs to be emphasized that this is a work in process, incomplete in some respects, and the SDT is very open to input on key issues. Indeed one of the slides each session presentation will include are open issues discovered since the draft was posted that the Team acknowledges need to be addressed going forward. This draft will not be what goes to ballot. It was suggested that participants should note if they see any "show stoppers" for their company. As an example, Sharon Edwards noted that the sub-team for Access Control struggled with the FERC directive to provide for "immediate" revocation. The Sub-team believes industry won't support what they cannot technically do.

Gerry Adamski committed to crafting a set of talking points which he will share with the Chair and Vice Chair to make sure all are on point and provide a consistent set of expectations with the workshop. The Team can review at the Tuesday walk through session. Scott Mix noted he would present some high-level concept ideas for some high level feedback regarding the implementation plan with help from a SDT drafting group.

Finally the Chair and Vice Chair both noted that a lot of members are getting push back from their companies in terms of the time commitment needed for working on this team. They requested that Gerry see if a note of thanks and appreciation from Jerry Cauley might be sent to SDT member companies.

B. "Parking Lot" Issues Raised in the Development of the Draft 010 and 011

During the final review of the draft CIP 010 and 011 in late April the SDT identified a number of issues that needed attention as the Team went forward with refining the draft. These were presented and discussed by the Team on Tuesday afternoon. Below is a table setting these issues out and how they were or will be resolved or handled going forward.

DRAFT CIP ~~VERSION 4~~ 010 & 011 "PARKING LOT"

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
Review clarity of item 1.1, Attachment 2 – Generation Facilities and criteria for Contingency Reserve and Reserve Sharing	Rich Kinas	4/29	CIP-010	**AI:** Revise item 1.1 with input from the industry through the informal comments received.
Shouldn't there be delegations made by the Senior Manager for any exceptions (CIP-011 R2 & R3)	Jackie Collett	4/29	Governance	**Resolved** by the revised CIP-011 text that was posted.
User type access (R3) 3.2 Review the need for network device training (Operators, etc.)	Jim Brenton	4/29	Physical/ Cyber & Access Control	Possibly regarding the level of access for outward facing and inward facing devices. What type of user training is required for each level? **Add role-based access (e.g., admin vs. application level access) – physical access & training requirements. Awareness training for everyone, and role-based training as required.**
Combine tables for electronic and physical access control systems (R6, R20, & R22)	Philip Huff	4/29	Physical and System Security	**AI:** Double-check that the proper requirements are incorporated in the respective tables.
Remove ~~Training~~ Termination for physical access to Low Impact (R9)	Doug Johnson	4/29	Physical	
What do the blank cells mean in the tables in instances where a timeframe is given? (R9)	Jackie Collette	4/29	Howard Gugel	Do they mean there is no requirement at that particular level? **AI:** Double-check the table entries to ensure that the entries are indicative of the requirement. Possibly a statement should be added to the Guidance Document that describes what is meant by a blank entry in a table.
Monitoring the baseline configuration means monitoring the physical location as written. (R23)	Rob Antonishen	4/29	Change Manage-ment (Dave Revill)	**AI:** Is baseline the right term? What do we mean by changing physical location?
What timeframe for issuing alerts (Table entry 18.2)	Jackie Collett	4/29	System Security	**AI:** What is the response time requirement? In what timeframe should the alerts be issued?
Need to address what disciplinary actions are? Should physical or cyber access be revoked?	Jackie Collett	5/11	Disciplinary actions (physical/cyber access)	AI:
Combine the revocation of physical and electronic access requirements (including remote access) into one topical area of the standard	Phil Huff	5/11/2010	Personnel access (Sharon Edwards)	**AI:** Need to investigate possible alternatives. Have a requirement to develop a procedure for handling revocation of access.

C. Development and Review of Sub-Team Workshop Presentations

The SDT reviewed and discussed initial sub-team draft presentations on Wednesday morning and agreed on some basic formatting. A template had been circulated to the sub-team leads before the meeting which was then modified during the initial review. The proposed slides included:

- Title slide with presenter name
- 2nd slide sub-team members and thanks to others participating
- Summary of requirements slide(s)
- Modification from Version 3 slide(s)
- Issues Identified since Posting
- Applicable FERC Directives and Requests for Interpretations
- Feedback sought at Technical Workshop
- Summary (optional)
- Questions

If possible and ready, the SDT would like to post the Change Mapping Tables along with the slides, but the slides are the priority. It was also pointed out that NERC advertised the technical workshop referencing "Draft Version 4," even though the proposed draft is 010 and 011. It should be made clear that this is a "work in process." The Team reviewed Scott Rosenberger's Recovery and Response slides as a way to review and discuss ways to increase consistency across the presentations.

Members offered the following comments on the presentation formats and approach:

- Sub-teams should use Scott's approach in terms of brevity.
- Important not to provide all the detail in the slides. We need a high level summary of the changes made with existing standard.
- In what order will it be presented? Present by sub-team or by topic? Proceed by topic.
- Identify Sub-team members and "special thanks"- to those helping the SDT? Contact each and check on their interest in being acknowledged.
- For the summary of requirements minimize the number of slides? Some have a single slide with requirements.
- Not more than 4 high level items per slide.
- Talking about CIP 010 and 011 don't reference "version"
- Issues Identified since Posting.
- FERC directives. Add requests for interpretation.
- On the Feedback slide(s)- highlight the key issues and questions.
- How long should presentations be? No more than 25-30 minute.
- Presentations will come first then handle the questions.

1. CYBER SECURITY ORDER 706 PROJECT 2008-06 – OVERVIEW AND APPROACH

Phil Huff presented the proposed opening slides that he and John Lim developed and would present together at the Workshop. Below is the final version of the presentation slides that were refined during two rounds of review with the SDT.

a. Final Overview and Approach Workshop Presentation Slides

OVERVIEW AND APPROACH

- Seeking Feedback on Proposed Draft- 2-Way Conversation
- This is a workshop- Not intended as training
- Draft is a work in progress- Not a finished product

INFORMAL COMMENT PROCESS

- New process approved by the Standards Committee--Receive feedback without the overhead of formally responding to every comment
- Focus on the requirements. Measures, Implementation Plan, VRFs and VSLs will be part of the formal posting
- January Informal Comment Response- 550 pages from 106 respondents (only 3 Requirements) – A record!
- Drafting Team can focus on making modifications to address comments

PROJECT 2008-06 SCOPE

- Address FERC Order 706 Directives
- Consideration of adapting the NIST Security Risk Management Framework
- Conform to latest version of ERO Rules of Procedure

REMAINING ORDER 706 DIRECTIVES

- 2 or more diverse security measures for defense in depth at the security boundaries
- Active vulnerability assessments every 3 years
- Incorporate forensic data collection and procedures

GUIDING PRINCIPLES

- Completeness
- Clarity
- Practicality
- Commensurate with BES impact
- Reduce Administrative Overhead
- Minimize the Need for TFEs
- Leverage Investment in Current Standard

GENERAL APPROACH

- Looked at NIST and other frameworks for suggestions and guidance
- Preserved some existing components of CIP-002 through CIP-009
- Requirements adapted from the DHS Catalog of Control Systems Security (subset of NIST 800-53)
- Includes directives from FERC Order 706

CIP 011 COMBINED REQUIREMENTS

- CIP-011 combines revisions and additions to CIP-003-3 through CIP-009-3

- Drafting Team requests feedback on the new CIP-011 format:
  - Keep CIP-011-1 as one document
    - Break CIP-011-1 up into multiple standards
    - No preference

NEW FEATURES-LOCAL DEFINITIONS

- New NERC Format
- Global definitions not always needed for area specific terms
- Improves readability by eliminating the need to look up terms in the Glossary

NEW FEATURES-TABLES

NEW FEATURES-OBJECTIVE STATEMENTS

- New NERC Format
- Provides a context to the requirement
- Maintains purpose throughout the development of requirements
- Assists in future interpretations

SCOPING-IMPACT CATEGORIZATION

- High Impact
  - Fewer BES Cyber Systems
  - High cost to implement and maintain
  - Moderate to significant reliability benefit
  - Highly capable security program
- Medium Impact
  - Moderate cost to implement and maintain
  - Moderate to significant reliability benefit
- Low Impact
  - Many more BES Cyber Systems
  - Moderate or minimal cost to implement and maintain
  - Moderate to significant reliability benefit
  - Lower cost to demonstrate compliance
  - Basic security program elements

COMPARISON- HIGH MEDIUM AND LOW

- High: Total requirements= 106
- Medium: Total requirements= 71
- Low: Total requirements= 22

SCOPING--CONNECTIVITY

- **External Connectivity** – A data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System.
- **Routable Protocol** – Communications protocol that contains a network address as well as a device address. It allows packets to be forwarded from one network to another.

- **Non-Routable Protocol** – Communications protocol that contains only a device address and not a network address. It does not incorporate an addressing scheme for sending data from one network to another.
- **External Connectivity a factor**:
  - Technical Requirements
- **External Connectivity NOT a factor**:
  - Most Organizational Requirements
  - Most Operational Requirements

SCOPING- OPERATIONAL ENVIRONMENT

Control Center

- Less distributed environment
- Easier to apply automated, traditional IT security controls.

Generation Facility

- Distributed cyber environment within a physical plant
- Longer system life-cycle
- Challenging test environment

Transmission Facility

- Highly distributed environment
- Difficult to automate security controls

TECHNICAL FEASIBILITY EXCEPTIONS

- Tried to write Standards at a higher level to minimize the need for TFEs
- Only FERC approved exception process to the Standards
- Looking for feedback on where to apply TFEs

GOVERNANCE REQUIREMENTS

- Policy focuses on high-level subject areas
  - Unnecessary to address every requirement in the policy
- Emergency provisions (exceptions) moved to appropriate requirements
- Removed policy exceptions

SCHEDULE FOR REVISION 4

COMMENTS

- Seeking **constructive comments**- Where you disagree, provide alternative language
- Provide context wherever possible
- Early comments are encouraged
- Comment response summary provided for July posting

SUMMARY

- Drafting team and industry developing Standards on an accelerated pace

- Applicability commensurate with BES impact
- Specifics of CIP-010 & CIP-011 will be presented during the remainder of the workshop

b. SDT Comments and Suggestions (2 rounds)

Overview and Approach Presentation Materials - 1st Round Comments and Suggestions

Did the industry see what kind of consideration was given for their comments on the concepts posted back in January 2010? The SDT posted a response to comment document with the draft 010 and 011 standards which addressed where comments resulted in changes.

- What about remaining post 010-011 issues?
- Requirement 22 (segmentation and separation) = 2 or more security measures for defense in depth at the security boundaries (related to network access) FERC 2 separate?
- Forensic
- Active vulnerability assessments every 3 years.
- Guiding Principles-Add Investments made- add
- CIP 11- Combined Requirements- Pros/Cons
- "Harder to manage document changes"? Overly broad statement.
- "Speak to challenge in reporting?" "Arbitrary renumbering of requirements?"
- Tracking requirements, documentation, policy and procedures around numbers.
- Cross reference linkages.
- Not helpful to say old standard was bad.
- Will refer to topics.
- CIP 11 is combined. Seeking comments.
- Describing the SDT thought process.
- Impact is how it impacts reliability on BES not on costs.
- Should focus on impacts to BES- not level of protection at H/M/L.
- Security requirements apply in terms of impacts to grid.
- "Most"
- Add slide? Environments, control centers, etc.
- Is connectivity defined?
- Looking for feedback on where it should apply.
- **"**Possible" 2nd and 3rd Ballot.
- Ballot pool formation

Overview and Approach Presentation Materials- 2nd Round Review and Comments

- Changes- shorter bullets based on 1st round suggestions.
- Every comment received will be read by the drafting team. Won't be responding to each in the informal comment round.
- Changed to CIP 01x from Version 4.
- Added guiding principles bullet: "Leverage investment in current standard"
- Took out advantages/disadvantages, pros/cons.
- Added a graphic providing a count for high, medium and low requirements.

- Consider adapting (vs. ~~adopting~~) the NIST framework? Yes
- Re-worded feasible language proposed by Jackie.

2. CYBER SECURITY ORDER 706 PROJECT 2008-06 – CIP-010 (FORMERLY CIP-002)

a. Final CIP 010 Workshop Presentation Slides

Jackie Collett presented the slides on behalf of the Sub-team (including Jim Brenton, Jay Cribb, Richard Kinas, John Lim, Dave Norton, David Revill, Scott Rosenberger, William Winters).

CIP 010 (FORMERLY CIP 002)

- Reliability Functions identified in the standard (Attachment I)
- Responsible Entity (Owner) identifies BES Cyber Systems performing Reliability Functions
- BES Cyber Systems are categorized (High / Medium / Low) based on BES Impact Criteria identified in the standard (Attachment II)
- Security requirements (controls) are applied based on BES Cyber System impact categorization (CIP-011)

DEFINITIONS

- **BES Cyber System Component**
  One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.
- **BES Cyber System**
  One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
- **Flexibility in defining BES Cyber Systems**

SUMMARY OF REQUIREMENTS

R1 - Identification of BES Cyber Systems

- Each Responsible Entity shall identify and document BES Cyber Systems It owns
- Cyber systems that execute or enable reliability functions- Functions identified in Attachment I
- **Scoping filter**

Functions Essential to Reliable Operation of the BES

- Identified in the standard (Attachment I)
- Essential to real-time reliable operation
- 15 minute window
- **Scoping filter:** Typically excludes business, market function systems, and non real-time systems

ATTACHMENT I: RELIABILITY FUNCTIONS

Functions Essential to Reliable Operation of the BES

- Dynamic Response
- Balancing Load and Generation
- Controlling frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring and Control
- Restoration of the BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

ATTACHMENT II: IMPACT CATEGORIZATION

BES Cyber Systems that impact

- **Generation Facilities:**
  - Contingency Reserve, total reserve sharing obligations
  - Real Power capability
  - Reliability "must run"
  - Blackstart Resources
- **Synchronous condensers, static VAR compensators and other Facilities not associated with Generation Facilities**
- **Transmission Facilities:**
  - • Transmission Lines
  - • Interconnections – major electric system networks
  - • Voltage Levels (Bulk Electric System)
  - • Primary Cranking Path (EOP-005)
  - • IROL violation, instability, uncontrolled separation or Cascading
  - • Loss of identified Generation Facilities
  - • Essential for Nuclear Plant Interface Requirements (NUC-001)
- **Special Protection Systems / Remedial Action Schemes**
- **Automatic aggregate load shed ≥ 300 MW**
- **Control Centers**
  - Primary and Backup

    Functions –
    - Reliability Coordinator
    - Balancing Authority
    - Transmission Operator
    - remotely control ≥ 2 Transmission substations / switching stations

R3 -REVIEW AND UPDATE CATEGORIZATION OF BES CYBER SYSTEMS

- Each Responsible Entity shall review and update the categorization of the BES Cyber Systems identified in R1
  - • within 36 months of last identification / categorization
  - • as result of planned change
- Update documentation within 45 days

DIFFERENCES FROM PREVIOUS VERSIONS

Version 1 / 2 / 3	Proposed CIP-010, CIP-011
Asset types to consider	Reliability Functions
Asset Identification Methodology	Asset threshold criteria
Critical Assets Cyber Assets Critical Cyber Assets	BES Cyber System Component BES Cyber Systems
Critical / Not Critical	BES Impact Levels – High / Medium / Low
"One Size Fits All" security	Security requirements commensurate with BES reliability impact
"All or nothing" security	All BES Cyber Systems will have some level of security (no NONE)

SIGNIFICANT CHANGES SINCE DRAFT CIP 002-4 POSTING

- No BES Subsystems / Generation Subsystems / Transmission Subsystems
  • *Response to comments to simplify*
- Impact categorization is applied directly to the BES Cyber System
  • Not inherited through BES Subsystem
- No provision for exclusion through an engineering evaluation approved by and oversight body (Reliability Coordinator or Regional Reliability Assurer)
  • Bright lines
  • Focus on BES Cyber Systems
  • *Response to comments received*

APPLICABLE FERC DIRECTIVES

FERC Order 706

- p322 – "… a mechanism for external review and approval of critical asset lists."
- p329 – "… to develop a process of external review and approval of critical asset lists based on a regional perspective."

Discrete, "bright line" BES Cyber System categorization criteria removes the need for external review and approval

FEEDBACK

- The Attachment I – Functions Essential to the Reliable Operation of the BES attempts to scope the cyber systems under consideration. What are possible issues with this approach? What changes would improve the identification of the **functions** essential to the reliable operation of the BES?
- The proposed definition of a **BES Cyber System** provides an entity flexibility in defining their specific BES Cyber Systems. What changes would improve the definition of a Cyber System?

- The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to **real-time** operations systems with an operational time horizon of **15 minutes**. Is the 15-minute time horizon appropriate for this standard? If not, what is an appropriate definition for "real-time" for the purposes of this standard?
- The proposed definition of **Control Center** attempts to characterize the cyber systems under consideration. What are possible issues with this approach? What changes would improve the definition of Control Center?
- Are the **impact categorization criteria** in Attachment II appropriate? What changes would improve the criteria?

SUMMARY

- BES Cyber Systems are scoped using both a functional and a 15 minute real-time criteria
- BES Cyber Systems are categorized based on their impact on the Bulk Electric System (High/Medium/Low)
- Security requirements will be applied according to BES Cyber System Impact categorization in CIP-011

a. SDT Comments and Suggestions (2 rounds)

CIP 010 Presentation Materials — 1st Round Comments and Suggestions

- Jackie Collett will present at the Workshop. Other Sub-Team Members will be there.
- Drew from a Presentation to Transmission Owners Forum last week for Dave Revill.
- Highlighted big pieces.
- Summary of Requirements R1. Use this as a template?
- What are the scoping filters?
- Attachment II- 1st hit list of what's in scope.
- BES cyber systems definition.
- Control center will be cleaned up.
- R3- no longer than 30 minutes?
- A little more time defining BES cyber systems. Bring up front so don't have to

CIP 010 Presentation Materials — 2nd Round Comments and Suggestions

- CIP 010. *(formerly CIP 002)*
- Definitions slide added.
- Differences from previous versions. New slide -comparison.
- Clarified critical assets, etc. High level-
- Discussion of how to conclude the presentation material.
- Place a note in the posting of the slides that there will be some formatting improvements ready for the workshops.
- What about a feedback question for attachment 1? Are they bright and drawn in the right place.
- Is the bright line in Attachment 1 bright enough? Jackie will review and redraft.
- Seek input on the changes will improve the draft

- What will be posted?
- Check on consistency- of the Change mapping.
- Put date on documents= footer and date of draft
- Data retention element- Issues ID- component, not an enforceable actionable element of standards. Will send extra slide.
- Incidence response standard- if you need requirement to hold data for some time for forensics investigation. In requirement section of incidence response.
- Moved all data retention to the compliance section. Did across the board by Maureen's suggestion.
- May have to fix this.
- If people want it make it part of the record. Won't be documented.
- Should we accept anonymous comments? No name. Accept?
- Probably will get some for legitimate business reasons (e.g. a vendor offering suggestions).

3. PERSONNEL AND PHYSICAL SECURITY (CIP-011 R2 – R6)

a. CIP 011 Final Presentation Materials- Personnel and Training and Physical Security

Doug Johnson presented the slides on behalf of the Sub-team (including Robert Antonishen, Patricio Leon-Alvarado and Kevin Sherlin).

SUMMARY OF REQUIREMENTS

Personnel Training, Awareness, and Risk Assessment

- R2 — Security Awareness Program
- R3 — Annual Cyber Security Training Program
- R4 — Personnel Risk Assessment

Physical Security

- R5 — Physical Security for BES Cyber Systems
- R6 — Physical Access Control Systems

MODIFICATIONS FROM VERSION 3

Personnel Training, Awareness, and Risk Assessment

- We have removed examples of how to do things, i.e. posters, emails, computer based training, etc., from the requirements and they will instead be part of guidance document(s)
- The single Access Control requirement (CIP-004-3 R4) was split into separate requirements in both the physical (R5) and electronic access control (R8 & R9) sections to eliminate the need to cross reference
- The intent is to only require the annual training and personnel risk assessment when a person is obtaining authorization for physical or electronic access

Physical Security

- Eliminated the Physical Security Perimeter term and concept

- We have removed examples of how to do things, i.e. card keys, special locks, electronic logs, video recording, manual logs, etc., from the requirements and they will instead be part of guidance document(s)
- We have separated when you need to restrict, monitor and log physical access to support varying controls needed for different impact levels or connectivity

ISSUES IDENTIFIED SINCE POSTING

- Physical Security requirement (R5) needs to better reference creation, update and review of physical security plan(s)
- Some additional electronic protections for physical security systems were inadvertently omitted (CIP-006-3 R2.2)
- The retention of log requirements are being moved to the Compliance Data Retention section (D.1.4) of the standard.
- Need to address FERC Order 706 par. 581, testing of physical security systems more frequently than every three years.

APPLICABLE FERC DIRECTIVES

FERC Order 706

- p434 – " …training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."
  - Addressed in 3.2
- p460 – " …immediate revocation of access privileges…"
  - Reduced the time to remove access in 5.8
- p581 – "…test the physical security measures on critical cyber assets more frequently than every three years."
  - Will need to be addressed in 6.4

Request for Interpretation

- RFI 2009-23 – Personnel Risk Assessment
  - Addressed in rewording of 4.1

FEEDBACK

Elimination of Physical Security Perimeter

- Do you support elimination of the Physical Security Perimeter term and introduction of the new multi level approach?

Frequency of physical security system testing

- Should the frequency of testing physical security systems be different based on environment? (i.e., control center, substation or generating station)

Time needed to revoke physical access

- FERC directed immediate revocation of access; what technical reasons or situations require additional time?

b. SDT Comments and Suggestions (2 rounds)

CIP 011 Presentation Materials — Personnel and Training and Physical Security 1st Round Comments and Suggestions

- Doug Johnson presented the materials for both personnel and training and physical security.
- Put interpretations as Well as FERC directives? Yes
- Removed at front of bullet.
- Requirement references where makes sense.
- ”or connectivity.” Where you need physical security for some mediums.
- Found some items needed to be revised, e.g. omitted electronic protection
- Reducing from 7 day- put FERC section number in document.
- “confirm your support”?
- Bullet the physical.

CIP 011 Presentation Materials- Personnel and Training and Physical Security 2nd Round

- Doug presented the materials for both personnel and training and physical security noting format changes, adding a new bullet to the FERC directives slide (p 581) and a new bullet on new bullet on FERC immediate revocation of access.

4. CYBER SECURITY ORDER 706 PROJECT 2008-06 – ELECTRONIC ACCESS CONTROL (R7 TO R14)

a. Final CIP 011 Electronic Access Control (R7-R14) Workshop Presentation Slides

Sharon Edwards presented the slides on behalf of the Sub-Team (including Jeff Hoffman and Frank Kim).

SUMMARY OF REQUIREMENTS

- Electronic Access Control (R7-R14) R7 – Account Management Specifications
- Defining BES Cyber System User/Group Account Types R8 – Account Management Implementation
- Authorization and Quarterly Review of Accounts. R9 – Local Electronic Access Revocation
- Timeframe varies based on Impact Level R10 – Account Access Control Specifications
- Password and Job Function-based Rights
- R11 – Wireless and Remote Electronic Access Documentation
    - Use Restrictions and Authorization
    - R12 – Wireless and Remote Electronic Access Management
        - Quarterly Review of Accounts
    - R13 – Remote Access Revocation
        - Timeframe varies based on Impact Level
    - R14 – Wireless and Remote Electronic Access Controls
        - Authentication Controls and Deny by Default

MODIFICATIONS FROM VERSION 3

New Requirements

- Identification of Account Types and Acceptable Use (R7)
- Wireless Controls and Access Management (R11)

Major Revisions from Version 3

- Shorten Timeframes for Revocation for Local and Remote Access (R9, R13)
- Consolidated Requirements for Logging into the System Security Section (R15-R19)

APPLICABLE FERC DIRECTIVES

FERC Order 706

Immediate Revocation

- p 460 - "… to require **immediate revocation** of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."
  - Timeframes have been shortened
    - Based on a **balance** between **regulatory directives** and industry **capability**
    - In consideration of the **risk** to the BES

FEEDBACK NEEDED THROUGH COMMENTS

Access Control Requirements are dispersed.

- Would it be preferable to see **all access control requirements** (to information, physical, and electronic access) in **one requirement**? (Q19)

Revised Access Revocation timeframes

- Given the regulatory directive, what changes would you recommend? (Q22)

Controls around Remote Access

- The SDT attempted to provide clarity around Remote Access
- Are there any additions or edits necessary to these requirements? (Q26)

SUMMARY FOR ELECTRONIC ACCESS CONTROL

Improvements in the Requirements

- New topics address **electronic access control documentation** and management for **wireless** technology
- Provide clarity around **remote access controls**
- Address **balance** between **FERC directives** for access control and **industry capabilities**

b. SDT Comments and Suggestions (2 rounds)

CIP 011 Presentation Materials- CIP 011 Electronic Access Control (R7-R14)1st Round Comments and Suggestions

- Under Modifications and Revisions. Put where that was done? Put in (parens).
- Log retention (try Retention of Logs) vs. log requirements.
- Given impact decided to quote the directive.

- Should we have summaries at the end of each presentation? Or a summary of all at the end? At end of each presentation.
- Q 22- add work revised access revocation.
- Add, Electronic Access Control R7-14
- Suggest adding: Access Requirements" in the slide title.

CIP 011 Presentation Materials- CIP 011 Electronic Access Control (R7-R14) 2nd Round

- Sharon presented the slides as revised based on the initial review and the Sub-team's review. The SDT accepted her sub-team's proposed changes.

5. CYBER SECURITY ORDER 706 PROJECT 2008-06 – SYSTEM SECURITY (R15-R19) AND BOUNDARY PROTECTION (R20-R22)

a. Final CIP 011 System Security (R15-R19) and Boundary Protection (R20-R22) Workshop Presentation Slides

Jay Cribb presented the slides on behalf of the Sub-team (which includes Jim Brenton, Jackie Collett, John Van Boxtel and John Varnell)

SUMMARY OF REQUIREMENTS

System Security (R15 – R19)

- R15 – Malicious Code
- R16 – Security Patch Management
- R17 – System Hardening
- R18 – Security Event Monitoring
- R19 – Communications and Data Integrity

Boundary Protection (R20 - R22)

- R20 – Electronic Boundary Protection
- R21 – System Boundary Protection
- R22 – Protective Cyber Systems

MODIFICATIONS FROM VERSION 3 SYSTEM SECURITY (R15 –R19)

R15 — Malicious Code

- Previously CIP-007 R4
- Simplification of wording regarding prevention and detection of malicious code
- To reduce need for TFE's
- **Medium** and **high impact** BES Cyber Systems

R16 — Security Patch Management

- Previously CIP-007 R3
- Requires a **fixed date** for application of **patches** or completion of **mitigation measures**.
- **Medium** and **high** impact BES Cyber Systems

R17 — System Hardening

- Previously CIP-007 R2 (and CIP-005 R2.2)
- Change to "**network accessible services**" for logical ports

- Addresses **physical ports** as well (FERC order)

R18 — Security Event Monitoring

- Previously CIP-007 R6
- Slight clarification and condensing of wording from previous standard
- Adds manual log review with time periods (FERC order)
- Only required on **medium** and **high** impact BES Cyber Systems

R19 — Communications and Data Integrity

- New requirement from DHS Catalog of Controls 2.8.8
- Objective – prevent use of **maliciously modified data** from impacting operation of the BES such as replay attacks, man-in-the-middle, etc
- Requires protection of data and communications that could impact operation of **externally connected High Impact BES Cyber Systems used in a Control Center**
- This requirement is very tricky to scope and we are seeking industry **comments** and **feedback**

MODIFICATIONS FROM VERSION 3 BOUNDARY PROTECTION (R20 –R22)

R20 — Electronic Boundary Protection

- Previously CIP-005 R1
- Changed wording to fit with BES Cyber Systems approach
- Adds requirement to **document** all digital communication paths **external** to the BES Cyber System
- Still requires establishing known access points and implementing access controls
- Still requires logging, alerting, and log review

R21— System Boundary Protection

- Objective - Limits scope of attack or propagation of compromise in a successful attack
- Only required on medium and high impact BES Cyber Systems
- Looking for industry comment and feedback

R22 — Protective Cyber Systems

- Previously CIP-005 R1.5 and CIP-006 R2.2
- Previously this was done through "Be afforded the protective measures specified in…"
- Changes scoping for protective and monitoring systems to only have a limited subset of the required measures
- Requirements scoped based on connectivity and BES Cyber System Impact Level

ISSUES IDENTIFIED SINCE POSTING

R17 — System Hardening

- May need scope review and additional criteria beyond ports and services such as default passwords (10.1) moved into this requirement
- System and Access Point Vulnerability Assessments

R18 — Security Event Monitoring

- Evaluating a maximum time period for responding to alerts

R22 — Protective Cyber Systems

- Reconcile with physical security systems and move to a separate group.

APPLICABLE FERC DIRECTIVES

FERC Order 706

- p511 — We are pointing to the remote access control requirements at each Electronic access point. Any further examples would be included in guidance documentation.
- p619, p622 — Reworded malware prevention requirements to require processes to detect the introduction of and prevent the propagation of malicious code.
- FERC Order in Docket RD10-3-000
- Included requirement to disable unused physical ports on BES Cyber System components.

FEEDBACK

- What is the appropriate scope for Communications Integrity requirement?
- What is the appropriate scope for System Boundary Protection requirement?
- Feedback on the Electronic Access Points concept.

b. SDT Comments and Suggestions (2 rounds)

CIP 011 System Security and Boundary Protection Presentation Materials- 1st Round- Comments and Suggestions

- Jay Cribb reviewed the proposed presentation slides with the SDT
- R17- first bullet? Will revisit and provide additional criteria.
- FERC Directives- note that examples will be in guidance documentation not in standard.
- Addressing physical ports- RD 10-3. Docket #
- Will create a feedback slide from the bullets scattered throughout.

CIP 011 System Security and Boundary Protection Presentation Materials — 2nd Round

- Modifications Slides — "Reduction in TFEs- "To reduce need for TFE's
- Issues identified since posting. Assessments added.
- Feedback- added from presentation.
- FERC directives- cross reference- overall, have all be addressed somewhere?
- Modification- system security (R 15-R19)
- Other areas for feedback. Where TFEs should be allowed? In intro slide.

6. CYBER SECURITY ORDER 706 PROJECT 2008-06 –CONFIGURATION CHANGE MANAGEMENT R23 INFORMATION PROTECTION & MEDIA SANITIZATION R24-R25 BES CYBER SYSTEM MAINTENANCE R26

a. Final CIP 011 System Security Configuration Change Management R23 Information Protection & Media Sanitization R24-R25 BES Cyber System Maintenance R26 Workshop Presentation Slides

Dave Revill presented on behalf of the Sub-Team (that included Keith Stouffer, Bill Winters, and Philip Huff)

SUMMARY OF REQUIREMENTS

Configuration Change Management (R23)

- R23: Prevent and detect unauthorized modifications to BES Cyber Systems

Information Protection & Media Sanitization (R24-R25)

- R24: Prevent unauthorized access to sensitive information associated with BES Cyber Systems
- R25: Prevent the unauthorized dissemination of BES Cyber System information.

BES Cyber System Maintenance (R26)

- R26: Prevent unauthorized maintenance on BES Cyber Systems and ensure that systems used for maintenance do not accidently introduce malicious code into the BES Cyber System.

CONFIGURATION CHANGE MANAGEMENT

- Inventory & Baseline Configuration (23.1, 23.2)
  - Additional items to track in the Medium & High categories (23.2)
- Changes to the inventory and baseline configuration trigger the change management process (23.3, 23.4)
- Assess potentially impacted cyber security controls (23.5)
- Test Environments for High Control Centers (23.6)
- Monitor & detect unauthorized changes (High) (23.7)

INFORMATION PROTECTION AND MEDIA SANITATION

- Local definition for sensitive information derived from CIP-003-3 R4.1
- Identification & classification of sensitive information (24.1)
- Labeling & handling procedures (24.2)
  - Handling would include procedures for items such as storage, transport, and disposal.
- Explicit authorization of access and revocation of access to sensitive information (24.3, 24.4)
- Verify authorizations every 12 months (24.5)
- Sanitization of media prior to disposal or reuse outside of BES Cyber Systems (25.1)

BES CYBER SYSTEM MAINTENANCE

- **Local definition of maintenance**
  - Devices temporarily connected to the BES Cyber System do not become a component of the BES Cyber System
- **Maintenance activities shall be performed by authorized personnel (26.1)**
- **Detect and prevent the introduction and propagation of malicious code on those devices used to perform maintenance (26.2)**

MODIFICATIONS FROM VERSION 3

- **Configuration Change Management**
  - Shift from “significant changes” (CIP-007-3 R1) to deviations from the baseline configuration and component inventory (23.3, 23.4)

- **Added to introduce clarity as to when the change management process should occur for compliance purposes**
- **Aligned with DHS Catalog of Control Systems Security, Section 2.6.2 Baseline Configuration**
  - Explicit requirement for testing environments in High Impact Control Centers (23.6)
- **Added in reference to FERC Order 706, paragraphs 609-611**
  - Monitoring for unauthorized changes for High Impact BES Cyber Systems (23.7)
- **Added in reference to FERC Order 706, paragraph 397**
- **Information Protection & Media Sanitization**
  - Introduction of labeling and handling procedures in order to clarify what is expected of the entity (CIP-003-3 R4, CIP-011-1 24.2)
  - Revocation of access to sensitive information within 24 hours for personnel terminated for cause (24.4)
- **Added in reference to FERC Order 706 paragraph 386**
  - Allowed for reuse of media amongst BES Cyber Systems (CIP-007-3 R7, CIP-011-1 25.1)
- **Added in reference to FERC Order 706 paragraph 633**
- **§BES Cyber System Maintenance (R26)**
  - New requirement inspired by the DHS Catalog of Control Systems Security (Section 2.10 System Development and Maintenance) in order to allow maintenance devices to be temporarily connected to the BES Cyber System

ISSUES IDENTIFIED SINCE POSTING

- The term "sensitive information" may be problematic for some entities who have a specific classification of information already designated as Sensitive. (R24)
- FERC Order 706 Paragraph 386 specifies that revocation of access to information should be prompt.
  - The proposed standards cover the situation of termination for cause, but currently does not address other types of termination, job change, etc. The drafting team will consider aligning revocation to information with the revocation of cyber and physical access to BES Cyber Systems. (24.4)
- Maintain consistency between requirements for malicious code prevention between maintenance devices and BES Cyber Systems (26.2, 15.2)

APPLICABLE FERC DIRECTIVES

CIP-011-1 24.5

- Revocation within 24 hours for personnel terminated for cause

FERC Order 706

- P386 "… to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done

so promptly. In general, the Commission … believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."

CIP-011-1 23.7

- Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes.

FERC Order 706

- p397 "…to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."

CIP-011-1 23.6

- Requires testing of changes in a test environment, documentation of differences between the test and production environments each time a change is performed, and measures to account for those differences

FERC Order 706

- §p609 "…to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. ...to consider providing further guidance on testing systems in a reference document."
- §p610 "…to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."
- §p611 "…the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."

CIP-011-1 25.1

- Sanitize the media in order to render the data unrecoverable

FERC Order 706

- p633 "…to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."
- p635 "… to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."

FEEDBACK

- Configuration Change Management
  - Component inventory and baseline configuration trigger for the change management process
- BES Cyber System Maintenance
  - Do you agree with the framework around BES Cyber System maintenance and maintenance devices?
  - What other requirements should be placed upon the maintenance devices?
- Provide feedback on whether the requirements are appropriate for each BES Cyber System impact level

b. SDT Comments and Suggestions (2 rounds)
Dave Revill presented on behalf of the Sub-Team (that included Keith Stouffer, Bill Winters, And Philip Huff)

CIP 011 Configuration Change Management R23 Information Protection & Media Sanitization R24-R25 BES Cyber System Maintenance R26 Presentation Materials- 1st Round Comments

BES Cyber System Maintenance

- Local definition of maintenance sub-bullet e.g.?
- In operations or under maintenance?
- "Prevent"?
- Put requirements 24.3. 15 didn't have prevent.
- 2nd bullet- "shall" vs "should."

Modifications from Version 3.

- Didn't have enough time in terms of h/m/l. configuration change management.
- Information Protection and Media Sanitation.
- BES Cyber System Maintenance.
- Physically connected only? No both that and remote.
- Consider this maintenance? Locally defined term.

Issues Identified Since Posting.

- Pick a word. Struggled with this issue at Entergy.
- "Prompt"- covered cause but not other things
- Revocation for suspension? This is a parking lot issue.

FERC Directives (several slides)

- Moving with FERC directives above?
- 2nd bullet-Feedback- slide. Technicians will be happy.

CIP 011 Configuration Change Management R23 Information Protection & Media Sanitization R24-R25 BES Cyber System Maintenance R26 Presentation Materials- 2nd Round

Dave Revill presented the following points on the revised presentation slides:

- 1st Slide- topical areas and Rs covered for consistency with others.
- Added R's as references
- Rows references were corrected.

7. CYBER SECURITY ORDER 706 PROJECT 2008-06 – CYBER SECURITY INCIDENT RESPONSE (R27 – R29) BES CYBER SYSTEM RECOVERY (R30 – R32)

a. Final CIP 011 Cyber Security Incident Response and Recovery Workshop Presentation Slides
Scott Rosenberger presented on behalf of the Sub-Team (that included Tom Stevenson and Joe Doetzl).

SUMMARY OF REQUIREMENTS

Cyber Security Incident Response (R27 – R29)

- Incident Response Plan (R27)
- Testing (R28)
- Review, Update, and Communication (R29)

BES Cyber System Recovery (R30 – R32)

- Recovery Plan (R30)
- Testing (R31)
- Review, Update, and Communication (R32)

MODIFICATIONS FROM VERSION 3

- Plan
- Testing
- Review, Update, and Communication
- Moved Training requirements to R3

Cyber Security Incident Response (R27 – R29)

- Included additional timing requirements on the update of response plan. (29.3,29.4)
- Included requirement for review after testing or actual response (29.1, 29.2)
- Added specific timing requirement on the communication of plan changes (29.5)

BES Cyber System Recovery (R30 – R32)

- Added requirements to additionally review plans after tests or actual events (R30, 32.1, 32.2, 32.3)
- Modified timing of testing based on Impact level. Added requirements for verifying backups and performing full operation tests once every 36 months (R31, 31.1, 31.2, 31.3)
- Added timing requirement on plan updates based on Impact level, added additional triggers that require plan updates (32.4, 32.5, 32.6, 32.7)
- Added testing of required information on backup media initially as well as every 12 months (31.2)

Added requirements related to restoration processes (*30.5)*

APPLICABLE FERC DIRECTIVES

Cyber Security Incident Response

- Covered in CIP-001 and Guidance
  - p661 – Definition of Incident, Guidance
  - p673 – Notification requirements (within 1 hr)

  - p676 - Notification requirements (within 1 hr)
- p686 - Maintain Documentation of Drills/Incidents including Lessons Learned

BES Cyber System Recovery

- p694 – RE's must implement a recovery plan
- p739 – Backups verified operational
- p748 – Backup are periodically verified usable

b. SDT Comments and Suggestions (2 rounds)

Scott presented the Sub-team's slides for review as a possible template for other Sub-Teams to use.

CIP 011 Cyber Security Incident Response and Recovery Presentation Materials- 1st Round
SDT Comments and Suggestions

- Liked the graphic depiction of H/M/L.
- Will reference rows without an "r"

CIP 011 Cyber Security Incident Response and Recovery Presentation Materials-2nd Round

- Scott Rosenberger noted the changes made in the slides made their format consistent with the other presentations.

IV. OTHER 706 ISSUES AND CIP DOCUMENT PREPARATION

A. Change Mapping and Addressing FERC Directives

Each Sub-team developed a table displaying the changes mapping from Version 3 to this version (See Appendix #10). The Table indicated: CIP Version 3 Requirements; CIP 010 or 011 Requirements; and DHS Catalogue of Controls reference if applicable; and a statement of changes to CIP and the rationale for the changes. The Sub-Teams agreed to create before the FERC/NERC meeting on May 27 a separate document noting how each Requirement addressed the FERC directives and interpretations.

B. FERC Order 706 Issues In Addition to CIP 010 and 011

The yeam discussed the FERC Order 706 issues that will be addressed by the SDT in 2011 following adoption of the CIP 010 and 011 Standards. Scott Mix reviewed a table with the remaining FERC directives. (See Appendix #9) He characterized these as 'up the 12 issues that are large, controversial and complicated' (e.g., multi-procedural defense in depth and forensics, etc.). Scott Mix suggested that at the Workshop the SDT should make it clear and obvious to the industry we have lopped off some big topics that will be addressed after finishing the current work.

SDT Discussion Points

- If industry has to jump through hoops now and then again after we come back with solutions on these additional issues, this will not be received well.
- The Team should reinforce that there are these "big Issues"
- We need to make clear, dedicate time to that. Industry doesn't understand what they will voting on doesn't include these big issues.

- We have to get information out sooner vs. later. Deserves more than just an honorable mention.
- Include in the next round of comments, perhaps in the July Comment form.
- We may need to annotate- this requirement could be affected by big issues.
- We have projects on smart grid. We keep changing the policy and other projects. WE need to let the industry catch up technologically. Waiting- what's going to happen next.
- If these are big things we can't do we have to put pressure back to government.
- 11 Items as big issues- 13 things to be done. Scott will prepare a short word document.
- Commission given direction- 706. NERC got a 1-time pass through December 2010. We have to assume unless directed otherwise, if we have been directed, we will do this.
- The unique nature of cyber security standards is that they are ever changing vs. other reliability standards with a long life cycle (e.g. weed management). The risk pictures are so dynamic, architectures have to be flexible to respond.
- The schedule has been filed by NERC and accepted FERC. Don't have the time or resources to address now. Not a lot of choice for the SDT. Have to address and make clear in the workshop.

C. Guidance Documents

The SDT discussed what kind of guidance documents the Team should be producing for industry implementation. Some members noted the value of guidance documents to help the industry understand the requirements.

On Thursday morning Mark Engels, Chair of the CIPC Working Group Control System for Security joined the Team and discussed their related work on developing consistency on when and how to draft of standards guidance documents. The Team indicated that they believed it would be very helpful to develop guidance documents in support of both 010 and 011. The Working Group is focused on helping SDTs with help in drafting specific supportive guidance documents. There was discussion on concerns in the delays in getting guidance documents on existing standards. Mark indicated that the Working Group would be open to a recommendation from the CSO 706 SDT regarding the need for the guidance and seeking assistance from the Working Group.

The Chair and Vice Chair noted that at the Sacramento meeting a Guidance drafting group would be formed.

D. Implementation Plan Concept and Team Schedule

Scott Mix presented the implementation plan concepts. *(See Appendix # 6)*

SDT Discussion Points

- Will this address "advanced implementation" by an entity? If 010 and 011- compliant with previous standards or pick a date and implement. Would there be an ability to change procedure so that entities could have option of complying of new standards in advance? Big question for NERC to answer.
- Roger Lampila noted that an entity making this choice would have to be compliant with 010 –it will be all or nothing. Roger agreed to put something together for NERC Compliance to respond to and bring back to the SDT.
- Compliance with both would be a nightmare.

- #3 & 4: if someone could do high in 2 years, could pull medium and low with them?
- Reinforce- this is pinned to risk. E.g. in policy and governance section.
- Not a 1-1 correlation? BES cyber system may be in vs. critical cyber assets.
- 1-6 cyber assets covered under CIP protection.
- There will be further refinement of concepts and a Team is forming.
- Provide High level thoughts at the Workshop? Scott Mix suggested an open q & a- if team comfortable.
- We will address points in the posted documents.
    - Implementation schedule. Factor in entity in terms timing re audit schedules so as not to waste money. Pick a date for highs. Entity should be free to decide to get done in terms of audit schedule.
    - Implementation plan- you will be compliant with 10 and 11 on this date. Or you can file with a plan prior to that date and will be held to it.
    - No longer audited for the previous standards.

V. NEXT STEPS AND ASSIGNMENTS

On Thursday the Team discussed the upcoming FERC/NERC meeting on May 27 where the SDT will be meeting with FERC staff in Washington D.C. to present the draft CIP standards and seek their initial feedback on the approach and the acceptability of the text.
The SDT discussed scheduling a preparation meeting of the SDT early in the week of May 24. Several SDT members indicated they were planning to be present for the session.

The team also discussed the Sacramento agenda and the likelihood of a very large volume of comments that the Team will have to read, review and decide how to respond and whether to adjust the drafts. It was agreed that after an overview of the responses from the Workshop and online Comments and review of the question of the 010 and 011 format, the sub-teams should plan on meeting Tuesday and Wednesday and report back to the full team on their recommendations.

Following the Sacramento meeting it was agreed there would be a need for weekly sub-team meetings and possible sub-team leads meetings. Later in June the schedule would be adjusted to reflect this and include some SDT meetings to develop drafts for NERC staff to review in advance of the July meeting in Pittsburgh.

The Chair thanked Scott Rosenberger for his excellent support for the SDT in hosting this meeting.

The meeting adjourned at 12:30 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- Review the CSO 706 SDT 2010 Work plan and Schedule;
- Review and adopt the CSO 706 SDT 2010 Consensus Procedures as refined;
- Receive updates on other related cyber security initiatives;
- Receive a NERC overview of the Technical Workshop;
- Review and Refine "Parking Lot" Issues from the April, 2010 CIP Documents for Informal Posting;
- Sub-Teams will: detail how FERC directives have been addressed; develop a "change documentation" draft; develop Technical Workshop Presentations; and identify possible guidance areas and bullet lists of guidance content;
- To review a proposal for drafting a CIP Guidance Document for posting in July, 2010;
- To review how the SDT will develop the CIP Measures, VSLs and VRFs for posting in July, 2010;
- To review the May 27, 2010 meeting with NERC/SDT and FERC; and
- Agree on next steps and assignments

Draft Agenda
Tuesday May 11, 2009

1:00 p.m.	Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines- *Joe Bucciero* Facilitator review and SDT acceptance of April 13-16, 2010 Atlanta SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review of April, 2010 Development of the Informal Documents for Posting- What Worked, What Could be Improved
1:30	Discussion of CSO 706 SDT Workplan, Schedule and Sub-team Expectations: May-December, 2010- *Stu Langton*
1:45	Review of Draft SDT Consensus Procedures
2:00	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
2:10	Technical Workshop Overview- Planning and Preparation- *Gerry Adamski?*
2:30	Review and Refine of "Parking Lot" Issues Draft from the April, 2010 Informal Posting Documents
3:00	*Break*
3:15	Review and Refine of "Parking Lot" Issues Draft from the April, 2010 Informal Posting Documents
4:45	Review of Expectations for Sub-Team Meetings on Wednesday
5:00	*Recess* ▪ *Possible Sub Team Meetings- Evening*

Wednesday	**May 12, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Security Controls Sub-Team Meetings Orientation and Expectations: • Detail how FERC directives have been addressed; • Develop a "change documentation" draft; • Develop Technical Workshop Presentations; • Identify possible guidance areas and bullet lists of guidance content; and • Begin to identify possible measures, VSLs and VRFs for Formal Comment posting in July.
8:30	Security Controls Sub-Team Meetings
10:30	Break
10:45	Security Controls Sub-Team Meetings
12:30	*Working Lunch*
1:15	Sub-Team Report CIP- 010- FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets
2:00	Sub-Team Reports CIP- 011 FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets
3:00	Break
3:15	Sub-Team Reports CIP- 011 FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets-*continued*
4:55	Review of Proposal for Thursday Agenda
5:00	*Recess* ▪ *Possible Sub Team Meetings- Evening*

Thursday	**May 13, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Sub-Team Reports CIP- 011 FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets-*continued*
10:00	*Break*
10:15	Review Proposal for a Guidance Document Drafting Team
10:30	Review How Measures, VSLs and VRFs will be Produced.
10:45	Review and Adopt SDT Consensus Procedures
11:00	Review May 27, 2010 NERC/SDT Meeting with FERC
11:15	Review of May 2010 Technical Workshop Planning and Preparation including Tuesday evening SDT Technical Workshop "Walk Through."
11:45	Review of Sacramento Agenda and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

Appendix # 2 Attendees List

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT (T/W/Th)
3. Jackie Collett	Manitoba Hydro
4. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
5. Doug Johnson	Exelon Corporation – Commonwealth Edison
6. Patricio Leon	Southern California Edison (T/W/Th)
7. John Lim, Chair	Consolidated Edison Co. NY
8. David Norton	Entergy (T/W/Th)
9. David S. Revill	Georgia Transmission Corporation
10. Scott Rosenberger	Luminant Energy (T/W/Th)
11. Jonathan Stanford	Bonneville Power Administration
12.Tom Stevenson	Constellation
13.Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
14. John Van Boxtel	WECC
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
Scott Mix	NERC
Roger Lampila	NERC
Howard Gugel	*NERC (Ready Talk/Phone) (T/W)*
Gerry Adamski	*NERC (Th) (Phone)*
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

16. Jay S. Cribb	Southern Company Services (T/W/Th)
17. Sharon Edwards	Duke Energy (T/W/Th)
18. Jeff Hoffman	U.S. Bureau of Reclamation, Denver (T/W/Th)
19. Frank Kim	Hydro One Networks Inc. (T/W/Th)
20. Rich Kinas	Orlando Utilities Commission (T)
21. Kevin Sherlin	Sacramento Municipal Utility District (W)
21. William Winters	Arizona Public Service, Inc. (T/W/Th)

SDT Members Not Participating

Joe Doetzl	Kansas City Pwr. & Light Co

Gerald S. Freese	America Electric Pwr.

Others Attending in Person

Mike Allgeier	LCRA
James Bassett	Invensys
Jim Fletcher	American Electric Power
Michael Keane	FERC
Brian Newell	American Electric Power
Bryn Wilson	OG&E
Guy Zito	NPCC

Others Attending via WebEx and Phone

May 11, 2010

Bill	Glynn	Westar Energy
Jerome	Farquharson	Burnsmcd
Tom	Beck	Florida Power and Light
Thomas	Brownback	FERC
Rod	Hardiman	Southern Company
Laura	Hussey	Selgs
Jan	Bargen	FECR
Andres	Lopez	US Army Corps of Engineersce.
Justin	Kelly	FERC
John	Fridye	RRI Energy
Steve	Newman	Midamerican
Maggy	Powell	Constellation Energy
Bill	Keagle	Constellation Energy

May 12, 2010

Jan Bargen	FERC
Jason Marshall	Midwest ISO
Rod Hardiman	Southern Company

May 13, 2010

Jason	Marshall	Midwest ISO
Bill	Glynn	Westar Energy
Jan	Bargen	FERC
Mark	Engels	Dominion Electric
John	Fridye	RRI Energy
Rod	Hardiman	Southern Company

Appendix #3 NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

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

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this

objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

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

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

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

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

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

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

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 4
MEETING SCHEDULE
APRIL–DECEMBER 2010

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	*Key Dates*	*CIP Task*
4/12/2010	**SDT Meeting Atlanta, GA (Southern Co) (4/13-16)**	**Present Controls draft for full SDT review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
4/19/2010	4/19-4/23/2010 4/23/2010	**SDT Sub-Teams and Leads Meet to Finalize Documents** **NERC Receives and Prepares Full Package for Industry Comment**
4/26/2010	**4/26/2010** **4/27/2010** **4/28/2010** **4/29/2010**	**SDT Sub-Teams Develop Package** **SDT Reviews with NERC Staff Proposals** **SDT Scoping Meeting on Documents** **SDT Reviews and Approves Full Package for 30-day Industry Comment Period**
5/3/2010	**5/4/2010**	**Informal Comment Posting for full package starts** **Completes on 6/3/2010**
5/10/2010	**SDT Meeting Dallas, TX (Luminant) (5/11-13)**	**Review Parking Lot Issues, Prepare for Industry Workshop and Begin Development of Guidance Documents**
5/17/2010	5/19 & 5/20/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
5/24/2010	5/24 to 5/28/2010 5/27/2010	**SDT Considers Comments from Workshop** **Meeting with FERC to Review Standards and Posting**
5/31/2010	6/3/2010 6/4/2010	**Informal comment period ends** **SDT Reviews Comments Received** **Sub team meetings to Review Comments Received**
6/7/2010	6/7/2010 **SDT Meeting, Sacramento, CA (SMUD) (6/8-11)**	**Sub team meetings to Review Comments Received** **Industry comment review, response process, re-drafting, as needed**
6/14/2010		Sub team meetings to prepare sections for review
6/21/2010	SDT Meeting and Subteams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review
6/28/2010	SDT Meeting and Subteams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review

Draft CSO706 SDT Schedule Page 1

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	*Key Dates*	*CIP Task*
7/5/2010	NERC Staff review	Sub teams complete all work assignments & NERC Review
7/12/2010	**SDT Meeting, Pittsburgh, PA (CERT) (7/13-16)**	**Finalize & Approve Documents for posting for 45 day formal comment period**
7/19/2010	7/19/2010 7/21/2010 7/21/2010	**-NERC seeks SC Approval for Ballot** **-Post CIP Standards for Formal Comment** **-45 Day formal comment period begins (closes on 9/3/2010)** **-Begin Ballot Pool Formation**
7/26/2010		**Formal comment period for CIP standards** **Prepare for industry webinar**
8/2/2010		**Formal comment period for CIP standards** **Prepare for industry webinar**
8/9/2010	**SDT Meeting, Chicago, IL (ComEd) (8/10-13)**	**Formal comment period for CIP standards** **Finalize presentation for industry webinar**
8/16/2010	8/17/2010 8/19/2010	**Hold Industry Webinar (tentative)** **Ballot Pool Formation Ends**
8/23/2010	8/25/2010	**Initial Ballot Begins**
8/30/2010	9/3/2010	**Initial Ballot Ends**
9/6/2010	**SDT Meeting Winnipeg, Canada (Manitoba Hydro) (9/7-10)**	**Review ballot results** **Respond to comments received** **Draft revisions to standards**
9/13/2010		Sub-team meetings
9/20/2010	9/20/2010 9/24/2010	Sub-team meetings, NERC Staff Review Full SDT on-line meeting to approve revised draft of documents for re-ballot
9/27/2010	9/27 to 10/6/2010	Re-Ballot Period
10/4/2010	10/6/2010	Re-Ballot ends; comments received by SDT

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	*Key Dates*	*CIP Task*
10/11/2010	**SDT Meeting, Toronto, Canada (OPG) (10/12-15)**	**Prepare responses to 2nd ballot comments**
10/18/2010		**Sub-teams meet to adjust requirements, as needed**
10/25/2010	10/25/2010 10/29/2010	**-Prepare and finalize revisions to standards** **-NERC Staff review** **-SDT Approval for re-ballot (if needed)**
11/1/2010	11/1 to 11/10/2010	3rd Ballot Period (if needed)
11/8/2010	11/10/2010	Ballot period ends
11/15/2010	**SDT Meeting, Baltimore, MD (Constellation Energy) (11/16-19)**	**Prepare responses to 3rd Ballot comments**
11/22/2010		*NERC and SDT finalize responses to ballot package*
11/29/2010		*Seek SC and BOT Approval for Filing*
12/6/2010		*Seek SC and BOT Approval for Filing*
12/13/2010	**SDT Meeting Tampa, FL (FRCC) (12/13-17)**	**SDT Meeting to review Filing Completion of Phase 2**
12/24/2010		***Submit for Regulatory Approval***

Appendix #5 SDT Consensus Procedures
Proposed Refined Consensus Guidelines (May, 2010)
(To be Reviewed at the May 11-13, 2010 CSO 706 SDT Meeting in Dallas, TX)

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

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

Postings for Industry Comment. For decisions on CIP standards documents to be posted for industry comment where the Team finds that 75% acceptance or support is not achievable but an option or options under consideration had greater than 50% support from the Team, the Team's accompanying Comment form will seek industry input to help the Team resolve any differences and select an option going forward.

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

Electronic Mail Voting. In order to include the full drafting team membership on key votes or in instances when a quorum is not present (in the room and/or on the phone), the Chair may call for a question to be decided by a vote of all SDT members by a subsequent email. Both notice of any electronic mail vote and the results of such votes will be conveyed to all SDT members.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator.

The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 75% super-majority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's

Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT Consensus Guidelines
Adopted Unanimously, November 13, 2008
Cyber Security for Order 706 Standard Drafting Team

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

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the Team finds that 100% acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in consensus ranking or vote on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51% of the appointed members being present (simple majority). The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the Team's adopted procedural guidelines, to make and approve motions; however, the 75% supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Team will utilize their adopted meeting guidelines for conduct during meetings. The Team will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

The presiding chair and/or Facilitator of the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by the Team's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that

may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair. In addition, in order to provide balance to the Team process, members agree to represent and consult with their stakeholder interest group.

Appendix #6 --Implementation Plan

SDT Implementation Plan Team (Lim, Collett, Johnson, Brenton, Stevenson, Mix)
The SDT is currently developing an Implementation Plan for these standards which will consider the following:

1. BES Cyber Systems categorized as High Impact which were previously designated as Critical Cyber Assets;
2. BES Cyber Systems categorized as High Impact which were NOT previously designated as Critical Cyber Assets;
3. BES Cyber Systems categorized as Medium Impact which were previously designated as Critical Cyber Assets;
4. BES Cyber Systems categorized as Medium Impact which were NOT previously designated as Critical Cyber Assets;
5. BES Cyber Systems categorized as Low Impact which were previously designated as Critical Cyber Assets;
6. BES Cyber Systems categorized as Low Impact which were NOT previously designated as Critical Cyber Assets;
7. New requirements not previously included in the CIP Version 1,2, and 3 standards, as they relate to the above categories;
8. Re-categorized BES Cyber Systems;
9. Nuclear Facilities.

A more straight-forward approach may be needed to ensure that all assets are accounted for in the process. Consider implementation plan requirements that minimize conflict with the audit schedule of the entities. Roger will check on the thoughts of the audit/compliance team at NERC and get back to the implementation team with their input.

Concepts:

1. **No** BW, SC, AC – only C dates
2. Based on FERC approval dates
3. High first, followed by medium, followed by low (2 yrs, 5 yrs, 10 yrs?)
4. “Short” time for high; “mid” time for medium; “long” time for low
5. Start medium after high is done; start low after medium is done?
6. By requirement?
7. Re-categorization – up vs. down
8. Re-categorization – by requirement?
9. Nuclear facilities – tied to NGP outages (like current plan) (need nuclear SME input)

“Advanced” implementation issue – will entities need to be compliant with both the current CIP standards while preparing to be compliant with the new CIP-010 and CIP-011 standards? (not individual requirements, and direction must be declared by the entity).

Appendix #7
Workshop Agenda
Draft Version 4 Critical Infrastructure Protection Standards
May 19-20, 2010 | Dallas, TX

Wednesday, May 19	
7:00 AM – 8:00 AM	Registration
8:00 AM – 8:15 AM	Introduction & Welcome *Gerry Adamski & Allen Mosher, Workshop Co-Chairs*
8:15 AM – 9:15 AM	CIP Overview and Approach *John Lim, Chair & Phil Huff, Vice-Chair*
9:15 AM – 10:45 AM	BES Cyber System Categorization *Jackie Collett, Manitoba Hydro*
10:45 AM – 11:00 AM	Coffee Break & Networking
11:00 AM – 12:00 PM	Personnel and Physical Security *Doug Johnson, Commonwealth Edison*
12:00 – 1:00 PM	Lunch
1:00 PM – 2:00 PM	Access Control *Sharon Edwards, Duke Energy*
2:00 PM – 3:00 PM	System Security and Boundary Protection *Jay Cribb, Southern Company Services*
3:00 PM – 3:30 PM	Coffee Break & Networking
3:30 PM – 4:30 PM	Configuration Change Management, Information Protection & Maintenance *David Revill, Georgia Transmission Corporation*
4:30 PM – 5:00 PM	Additional Q&A and Daily Wrap-Up *John Lim, Chair & Phil Huff, Vice-Chair*
5:00 PM – 6:00 PM	Individual discussions with Drafting Team members – over cocktails and snacks from the hotel reception

Thursday, May 20	
8:00 AM – 8:10 AM	Introduction & Welcome *Gerry Adamski & Allen Mosher, Workshop Co-Chairs*
8:10 AM – 8:30 AM	Review of Workshop Day 1 *John Lim, Chair & Phil Huff, Vice-Chair*
8:30 AM – 9:30 AM	Recovery and Response *Scott Rosenberger, Luminant*
9:30 AM – 10:00 AM	Coffee Break & Networking
10:00 AM – 11:00 AM	Open Question and Answer, *All*
11:00 AM – 12:00 PM	Workshop Wrap-Up John Lim, Chair & Phil Huff, Vice-Chair
12:00 PM	Adjourn

Appendix #8
CSO 706 SDT DRAFTING SUB-TEAMS AND PRINCIPLES

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

Security Controls Sub-Team Principles and Drafting Guidance
CSO 706 SDT SECURITY CONTROLS SUB-TEAM DRAFTING PRINCIPLES
(ADOPTED BY CSO 706 SDT, JANUARY, 2010)

1. Applicability [NERC ROP] Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted.	**9.Practicality** [NERC ROP] **–** Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
2. Reliabiliy Objective [NERC ROP] Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system.	**10. Consistent Terminology** [NERC ROP] To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.
3. Performance Requirement or Outcome (NERC ROP) Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest.	**11. Commensurate Controls for BES Impact Categories.** Security controls shall be commensurate with the identified level of BES impact categories.
4. Measurability (ROP) Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement.	**12. Change Documentation.** Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes: a. Above and beyond the current standards; b. Removal of requirements; and c. Major formatting changes.
5.Technical Basis in Engineering and Operations [NERC ROP] Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.	**13. Reduce Administrative Overhead**. Administrative documentation shall be kept to the minimum that is necessary
6. Completeness (NERC ROP) Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.	**14. Priority.** Implementation plans for the Standards are prioritized according to level of BES impact.
7. Consequences for Non-Compliance [NERC ROP] In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.	**15. Eliminate or Minimize TFEs.** Security controls shall eliminate or at least minimize the need for TFEs. Allow for compensating controls to mitigate the need for a TFE.
8. Clear Language [NERC ROP] – Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.	

SECURITY CONTROLS SUB-TEAM
PROCESS AND DRAFTING GUIDANCE AND DELIVERABLES
Guidance from the January, 2010 Tucker Meeting and the February 2010 Austin Meeting

For the purpose of maintaining consistency across the teams and capturing interim decisions and change documentation, each team should utilize the following development process:

1. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
2. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
3. **Specific not Prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
4. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
5. **Develop the requirement language** for each security control identified in step 1.
   a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
   b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog.*
6. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
7. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
8. **Address specific directives from FERC Order 706** that may be applicable to the requirement.
9. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, consider the cost in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
10. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
11. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.
    (c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.
12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.

APPENDIX # 9
FERC 706 DIRECTIVES THAT WILL NEED TO BE ADDRESSED FOLLOWING VERSION 4

Paragraph	Text	Version/Approach	Status
13	NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.	Versions 2, 3, 4, post-4 Standards Development	NERC will update its timeline for addressing Order No. 706 directives in its filings for Versions 3, 4, and post-4 of the project. Each version will include a new or revised Implementation Plan.
89	We direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule	Versions 2, 3, 4, post-4 Standards Development	NERC will update its timeline for addressing Order No. 706 directives in its filings for Versions 3, 4, and post-4 of the project. Each version will include a new or revised Implementation Plan.
496	The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter	Post Version 4	
502	The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.	Post Version 4	

502	The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Post Version 4 Guideline – who would get assigned the development of this guideline?	
503	The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures.	Post Version 4	
547	We direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	Post Version 4 – Standards Development	.
572	The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets.	Post Version 4	
575	The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Post Version 4 Guideline – who would get assigned the development of this guideline?	

643	The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.	Post Version 4 Guideline – sounds like some of this information might be included in a guideline? Thoughts?	
706	The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.	Post Version 4	
710	Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report.	Post Version 4	
725	The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.	Post Version 4	

Appendix #10 CIP Mapping and Change Documentation

CIP MAPPING AND CHANGE DOCUMENTATION- CIP 010

NERC CIP-002 Std. Requirement	*CIP-010-1 Requirement*	*DHS Catalogue Reference (If Applicable)*	*Changes to CIP*	*Rationale*
002 R1	*R1*		*Critical Asset Identification Method is replaced by criteria in Attachment 2. R1 in CIP-010 now requires identification of all BES Cyber Systems based on functions in attachment 1 and real-time impact on BES reliability and operation.*	*A more deterministic impact assessment method based on thresholds and bright lines for more consistent identification of BES Cyber Systems. Addresses FERC directive on oversight of Critical Assets.*
002 R2, R3	*R2*		*Identification of Critical Assets is no longer required. Now requires categorization of BES Cyber Systems identified in R1 based on impact criteria in Attachment 2. CIP-002 R3.1, 3.2 and 3.3 no longer apply.*	*More direct evaluation of the impact of BES Cyber Systems based on functions.*
002 R4	*R3*		*Review required every 36 months and updates within 45 days of change*	*New requirement to update for changes in*

CIP MAPPING AND CHANGE DOCUMENTATION-PERSONNEL AND PHYSICAL SECURITY

NERC CIP-4-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
004 R1.	011 R2.		Minor wording changes	Effectively unchanged
004 R2.	011 R3.		Minor wording changes	Effectively unchanged
004 R2.1.	011 R3.		Minor wording changes	Modified to address FERC Order 706 directive par 443.
004 R2.2.	011 R3.1.		Minor wording changes	Effectively unchanged
004 R2.2.1.	011 R3.1.		Minor wording changes	Effectively unchanged
004 R2.2.2.	011 R3.1.		Minor wording changes	Changed to specify minimum required training to address FERC Order 706 directive par 433.
004 R2.2.3.	011 R3.1.		Requirement has been expanded to include storage media and visitor control program	To include storage media and ensure personnel with physical access understands the visitor control program
-	011 R3.2		New requirement	Added to address FERC Order 706 directive par 434
004 R2.2.4.	011 R3.3, R3.4		Requirement has been separated into two	For clarification
004 R2.3.	011 R3.5.		Minor wording changes	Effectively unchanged
004 R3.	011 R4.		Minor wording changes	Modified to address FERC Order 706 directive par 443.
004 R3.1.	011 R4.1.		Minor wording changes	Updated to address Request for Interpretation 2009-23.

NERC CIP-4-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
004 R3.2.	011 R4.3.		Minor wording changes	Effectively unchanged
004 R3.3.	011 R4.2.		Minor wording changes	Effectively unchanged
004 R4.	011 R5 for physical accsess, 011 R9 for electronic access, 011 R13 for remote access		This was split into separate physical and electronic access control requirements with the removal of the need to maintain a list(s)	So all physical or electronic access control requirements are grouped together.
004 R4.1.	011 R5 for physical accsess, 011 R9 for electronic access, 011 R13 for remote access		This was split into separate physical and electronic access control requirements	So all physical or electronic access control requirements are grouped together.

NERC CIP-4-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
004 R4.2.	011 R5 for physical accsess, 011 R9 for electronic access, 011 R13 for remote access		This was split into separate physical and electronic access control requirements and revoking time has been categorized per system impact, environment and cause.	Reduce revoking time to address FERC Order 706 Directive

CIP MAPPING AND CHANGE DOCUMENTATION- ELECTRONIC ACCESS CONTROL

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
004 R4	7.1 (account types)	2.15.3.1-3	Separate document listing account types is no longer required, but the information is still required (included in the system)	Maintaining a separate list does not increase system security
004 R4.1	8.2 (account), 12.1(remote)	2.15.3.1-6	Requires quarterly review of remote access accounts	Clarity for definition of those who have access Eliminate un-needed remote access
004 R4.2	R9(account), R13(remote)	2.15.3.1-8	Shortened revocation timeframes Specified timeframe for remote access revocation	FERC Directive in Order 706 Risk to reliable operation of the BES
007 R5	R10 (account), R14 (remote)		Controls are more explicitly defined	Minimize confusion concerning controls for remote access
007 R5.1	10.6 & 10.7 (account), R14 (remote)	2.15.3.1-9	Require authorization permissions to minimize access privileges as necessary to perform work functions Require explicit authorization access to system and security administrative functions	Permissions should provide the minimum access privileges necessary to perform work functions
007 R5.1.1	8.2 (account), 12.1(remote)		Implement a quarterly review of personnel access	Assurance that user accounts are implemented as approved via use of quarterly review
007 R5.1.2	N/A		Grouped all of the log requirements in operations security	More logical grouping of requirements
007 R5.1.3	8.2 (account), 12.1(remote)		Require quarterly reviews	Accounts need to be reviewed quarterly. Simplify the requirements for account reviews

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
007 R5.2	10.1		Change default vendor passwords after installation of vendor provided devices and systems	Definition of a more specific requirement
007 R5.2.1	10.1(Review)		Change default vendor passwords after installation of vendor provided devices and systems	Definition of a more specific requirement
007 R5.2.2	7.1, 7.2		Require documentation of acceptable use of such accounts	Definition of acceptable use of shared accounts
007 R5.2.3	8.1, 8.3, R9		Reorganized requirements for clarity	Achieve better clarity
007 R5.3, R5.3.1, R5.3.2	10.3, 10.4, 10.5		Provided flexibility to account for limitations of equipment capabilities	Account for equipment technical capabilities
007 R5.3.3	10.2		Changed annually to at least once every 12 months	Clarity for an annual review requirement

CIP MAPPING AND CHANGE DOCUMENTATION-
SYSTEM SECURITY AND BOUNDARY PROTECTION

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
007 R4	R15		Changes wording to be less prescriptive in prevention of malicious code.	Prevents TFEs for Antivirus/Antimalware software
007 R3	R16		Slight wording changes from previous standard mainly to require that you must have a fixed date for application for patch or completion of mitigation measures.	Effectively unchanged
007 R2 005 R2.2	R17		Slight wording changes from previous standard	Effectively unchanged
007 R3	R18		Slight wording changes from previous standard mainly to require that you must have a fixed date for application for patch or completion of mitigation measures	Effectively unchanged
	R19	2.8.8	Addition from DHS 2.8.8 - Communication Integrity	Need to try and protect High Impact BES Cyber Systems from data tampering and replay attacks
005 R1 005 R3	R20	2.8.7	Changed based on BES Cyber Systems and to define boundaries as systems and components outside of an entities defined BES Cyber System.	Needed to fit with change from Critical Assets and Critical Cyber Assets to protection of BES Cyber Systems
	R21	2.8.3	Addition from DHS 2.8.3 - Security Function Isolation	Limits scope of attack or propagation of compromise in a successful attack

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
005 R1.5 006 R2.2	R22		Previously this was done through "Be afforded the protective measures specified in…"	Changes scoping for protective and monitoring systems to only have a limited subset of the required measures.
005 R1.1 005 R1.2 005 R1.3 005 R1.4			Removed	These were all definitions in nature, not true requirements. The concerns are handled by the Electronic Access Point concept in CIP-011 R20.
005 R1.6			Removed	Moving to the BES Cyber System concept handled this requirement. BES Cyber System inventories are required in R23 and access points are documented in R20.

CIP MAPPING AND CHANGE DOCUMENTATION-CONFIGURATION CHANGE MANAGEMENT, INFORMATION PROTECTION MAINTENANCE

NERC CIP-3 Std. Requirement	*CIP-011-1 Requirement*	*DHS Catalogue Reference (If Applicable)*	*Changes to CIP*	*Rationale*
003 R4	*R24, R24.2*		*Removed the introductory requirement reference to a program for protecting information associated with Critical Cyber Assets. The introductory text now only requires documentation and implementation of procedures that incorporate the criteria in the table.*	*It is unclear whether a "program" implies additional requirements for the Responsible Entity. Any implied requirements should be explicitly included in the table (i.e. labeling & handling procedures).*
003 R4.1	*Local Definition*		*Incorporated the scoping of information to be protected within the local definition of "sensitive information".*	*The requirement only defined the type of information needed to be protected.*
003 R4.2	*TB 24.1*		*Minor wording changes*	*Wording changes to change the scope of the information from Critical Cyber Assets to BES Cyber Systems*
003 R4.3	*R1*		*Removed.*	*The entity is already responsible for continuous compliance monitoring of its information protection program.*
003 R5	*TB 24.2, 24.3, 24.4, 24.5*		*Access control is covered through requirements for handling, access authorization, and access revocation.*	*It is unclear whether a "program" implies additional requirements for the Responsible Entity. Any implied requirements should be explicitly included in the table.*
003 R5.1	*R1*		*Moved to Governance (R1)*	*The Responsible Entity is already required to have roles and responsibilities for authorizing access as part of their security policy in the Governance section of CIP-011.*

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
003 R5.1.1	R1		Moved to Governance (R1)	Identifying authorizing personnel by name, title and information type is an administrative requirement only. Governance requires identification of roles and responsibilities.
003 R5.1.2	R1		Moved to Governance (R1)	An annual review of the policy, including roles and responsibilities, is already required for the security policy in the Governance section of CIP-011.
003 R5.2	TB 24.3 and 24.5		Added the requirement to explicitly authorize personnel for access to sensitive information and review these access privileges annually.	Annually reviewing access privileges to protected information is an implication of the information protection "program". This requirement is now explicitly stated in the table. An annual review of access privileges is part of 24.5.
003 R5.3	N/A		Removed.	This requires a review of an access privilege enforcement process that is not defined anywhere within the Standard. It was removed for clarity. There is still a requirement to verify annually that the access privileges reflect authorization.
003 R6	R23, TB 23.3,TB 23.4		Wording changes for clarity	Provide clarity on when and how to perform configuration change management.
007 R1	TB 23.5		Essentially none	Transitioned from significant changes to changes that deviate from the baseline to add clarity to when testing needs to be performed.
007 R1.1	N/A		Removed.	This requirement is an administrative step in the process of assessing potentially impacted cyber security controls and testing changes to the BES Cyber System and was removed.

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
007 R1.2	TB 23.6		The revised standard requires a test environment for high control centers. In addition, it requires that differences between the test environment and the production environment are documented and measures are taken to account for those differences.	The test environment and associated documentation was added in response to FERC Order 706 paragraphs 609-611.
007 R1.3	TB 23.6		Essentially none.	
007 R7	R25		Essentially none.	
007 R7.1	TB 25.1		Changed "destroy or erase" to sanitize in order to render the data unrecoverable	Modified in response to FERC Order 706, paragraph 633 and 635.
007 R7.2	TB 25.1		Allowed for redeployment within BES Cyber Systems	The media is still under the scope of the CIP standards within the same entity.
007 R7.3	N/A		Removed	This is an administrative requirement that will be covered under proper demonstration of TB 25.1.
N/A	TB 23.1		New requirement	Concept taken from the DHS Catalog of Control Systems Security, Section 2.6.2 Baseline Configuration in order to have an easily identifiable set of attributes that could be used to determine exactly when the configuration change management process would be required.
N/A	TB 23.2		New requirement	Concept taken from the DHS Catalog of Control Systems Security, Section 2.6.2 Baseline Configuration in order to have an easily identifiable set of attributes that could be used to determine exactly when the configuration change management process would be required.

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
N/A	TB 23.7		New requirement	Response to FERC Order paragraph 397 "to consider accidental consequences and malicious actions along with intentional changes"
N/A	R26		New requirement	New requirement inspired by the DHS Catalog of Control Systems Security, Section 2.10 System Development and Maintenance
N/A	TB26.1		New requirement	Inspired by DHS Catalog of Control Systems Security, Section 2.10 System Development and Maintenance in order to ensure that maintenance to BES Cyber Systems is performed by authorized personnel.
N/A	TB26.2		New requirement	Inspired by DHS Catalog of Control Systems Security, Section 2.10 System Development and Maintenance in order to account for those systems used for maintenance that need to be temporarily connected to the BES Cyber System.

CIP MAPPING AND CHANGE DOCUMENTATION-RESPONSE & RECOVERY

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
008 R1	R27		Minor wording changes	Effectively unchanged
008 R1.1	R27.1		Minor wording changes	Effectively unchanged
008 R1.2	R27.2		Minor wording changes	Effectively unchanged
008 R1.3	R27.3		Minor wording changes	Effectively unchanged
008 R1.4	R29.3,R29.4		Included additional specification on update of response plan.	Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls
008 R1.5	R29.1 R29.2		Included requirement for review after testing or actual response	Based on review of DHS Controls
008 R1.6	R28		Minor wording changes	Effectively unchanged
	R29.5		Added specific timing requirement on communication of plan changes	Based on review of DHS Controls
009 R1	R30, R32.1, R32.2, R32.3		Added the requirements to additionally review plans after tests or actual events based on Impact level	Addresses FERC Requirement (694) to Implement recovery plans and aspects of the DHS Controls
009 R1.1	R30.1, R30.3		Minor wording changes	Effectively unchanged
009 R1.2	R30.2		Minor wording changes	Effectively unchanged

NERC CIP-3 Std. Requirement	CIP-011-1 Requirement	DHS Catalogue Reference (If Applicable)	Changes to CIP	Rationale
009 R2	R31, R31.1, R31.2, R31.3		Modified timing of testing based on Impact level. Added requirements for verifying backups and performing full operation tests once every 36 months	Addresses FERC Requirements (739, 748) related to testing of backups
009 R3	R32.4, R32,5, R32.6, R32.7		Added timing requirement on plan updates based on Impact level, added additional changes that require plan updates	Based on review of DHS Controls
009 R4	R30.4,		Minor wording changes	Effectively unchanged
009 R5	R31.2		Requires testing of required information on backup media initially as well	Based on review of DHS Controls
	R30.5		Added requirements related to restoration processes	Based on review of DHS Controls