NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes

Cyber Security Order 706 SDT — Project 2008-06

March 9, 2010 I 1 PM to 5 PM EDT
March 10, 2010 | 8 AM to 5 PM EDT
March 11, 2010 | 8 AM to 5 PM EDT
March 12, 2010 | 8 AM to 1 PM EDT

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 March 9-12, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT MARCH 9-12, 2010 MEETING
EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, John Lim welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The host Bill Winters, a SDT member, welcomed everyone to the facilities and covered logistics. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. On Friday morning the SDT approved without objection the meeting summary for the February, 2010 SDT session in Austin Texas. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines.

He suggested the Team was at a crossroads in terms of getting some of our product out to the industry and getting beyond conceptual discussions. He noted we need to have complete draft CIP package at the end of our April Meeting for posting for informal comment in early May. He suggested the focus needed to be on getting things done and that once the SDT has agreed then it needed to move forward and not revisit previous discussions.

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials. On day two, Stu Langton reviewed the SDT schedule sent out yesterday from Scott Mix. He noted that this is our 20th meeting over past eighteen months and the SDT has faced four core challenges:

- Over 200 items in 706;
- High visibility issue in the industry and Congress;
- Large team formed in effort to represent points of view of the industry; and
- Two different cultures addressing cyber security-- engineering/production backgrounds and engineering/cyber security backgrounds.

John Lim introduced Carl Dombek the new NERC communications director and asked him for a progress report on the communication plan for the drafting team activities and drafting of the standards.

On Wednesday, Howard Gugel, NERC, presented an overview with guidance for the Team on drafting standards and requirements which he and Maureen prepared. He noted the overall move towards performance based standards and described the general process for writing a standard. He suggested starting with the end in mind and FERC's criteria for approval:

- Achieves a specified reliability goal,
- Is applicable to all regions and entities, and

- Considers costs but not at expense of reliability.

It is important for the Team to build consensus at every step. As the Team has experienced first hand this is most difficult to develop at the concepts and assumptions level first, before addressing the drafting of requirements, then measures and compliance element.

John Lim provided a progress report on the Subteam's work since Austin noting that Dave Revill has worked on a strawman set of requirements to work with using criteria posted as a starting point. Jackie has done some more work on Attachment #2. John reviewed with the Team the following issues the CIP 002 Sub-team has been grappling with:

- Definitions
- Drafting Language
- Control room vs. control center.
- Legacy.
- Multiple facilities.
- Control system.
- Added 4.1.10 Distribution Provider (with qualification)

Dave Revill presented the concept of breaking requirements into two components:
1.1 Uniquely identify and document assets
1.2 Identify types of data communication into five technologies: routable, non-routable, dial-up, serial or not networked
- Definitions build on the attachment
- Created matrix using the five categories of communication technology including:
- And assigned high-medium-low as compared with BES impact rating

John Lim then presented an overview of the approach taken in the attachments and the SDT discussed the following issues:
- Real Time
- Audits, Standards and Guidance
- Functions.
- Disturbance to the BES.
- Addressing Industry Comments.

During the course of the first day's discussion a number of issues were noted in a "parking lot" for sub-teams to return to. Based on a review of the parking lot issues, the Team agreed to the following drafting assignments over night:
- Control System – Produce a list of examples
- Matrix Group – "connected/not connected"
- Real Time Operation/Cyber System affecting "immediate impact"

- Attachment 2 – guidance, matrix

The drafting groups then reported back to the SDT on Wednesday morning. Following their reports the SDT tested the level of support for the following guidance for the CIP 002 sub-team

1. Redraft CIP-002 to remove the connectivity options and handle them in the controls
   Y= 15 N = 5
2. Keep CIP-002 as drafted yesterday and let cip-002 sub-team handle modifications to the matrix (Austin)
   Y= 4 N= 16

The Team acknowledged they may need to revisit if in developing controls we find we cannot address the connectivity issue.

John Lim reported on Thursday the Sub-Team's efforts. On Friday the Sub-team reported on the changes made to the requirements and attachments.

- BES Cyber System definition
- Control Center
- Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced: Critical Assets; Critical Cyber Assets; Cyber Assets.
- The inclusion of Distribution Provider remains an open issue.
- "Multiple locations" definition- concerns whether it is needed?
- "Cyber security definition"?
- Distribution provider?
- R1-3. If 2 requirements
- Attachment #1 included a list of functions which the SDT reviewed and suggested refinements
- Attachment #2 provided a draft list of high, medium and low impact ratings which the SDT reviewed and suggested refinements.

On Wednesday the Sub-teams presented brief status reports before breaking into sub-team meetings. On Thursday each Sub-Team presented their draft requirements.

Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson(Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin

The Sub-Team report was delivered by Doug Johnson and covered drafting on the following areas:

- Personnel
- Awareness programs
- Training
- Personnel Risk Assessment
- Physical
- Physical Security Plan
- Physical Access Control
- Monitoring Physical Access
- Logging
- Visitor Control Program
- Maintenance and Testing
- Protection of Electronic Access Control Systems

Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl,

Scott Rosenberger reported on the Sub-team's progress reviewing draft language covering:

- Response
- Recovery Plans CIP 009
- DHS New Requirements

Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*

Sharon Edwards reported on the Sub-team's work including update on work, future tasks for the sub-team and areas of coordination with other Sub-teams.

Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Dave Revill, Phil Huff (Lead) *Observer Participants: John Fridye*

Phil Huff reported on the Sub-Team's work reviewing the Change Management requirements worksheet. He noted that the Sub-team's work focused on the language itself, not on applicability. They still have to go through FERC order review. The have modified table/worksheet to track open issues/complications. They now have drafted most of the objectives and changes to CIP language and covered:

- Baseline Configuration
- Configuration control
- Access restrictions for configuration changes.
- Configuration assets-
- Information Protection
- Protection Program.
- Maintenance
- Media protection CIP 7 R7-

Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell

Jay Cribb reported on this group's effort covering:

- Boundary Protection/ESP
- Electronic Access Monitoring.
- Communications Integrity
- Remote and Accessible Services (Port and Services)
- Flaw Remediation (i.e. DHS for Patch Management)
- Malicious Software Prevention.

Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton

Jon Stanford reported on the Sub-Team's work reviewing the Requirements Worksheet. He noted that the right hand side includes the current CIP and covered:

- Security Policy and Procedures
- Control System Security Plan
- Security Plan Update
- Control System Connections
- Vulnerability Assessment and Awareness.

The SDT reviewed the plans for the May 2010 Technical Workshop including Gerry Adamski's email. Gerry Adamski has offered to be the "general facilitator" for the workshop.

The Chair and Vice Chair noted that the Team had made a lot of progress over the course of the meeting. They reviewed the short term schedule for the Sub-teams. They will be meeting weekly as will the Sub-Team Leads to help coordinate the development of the drafts. There is a lot of work to complete. Sub-teams may be scheduling additional working sessions and coordinating with Joe Bucierro. The SDT needs to enter its April meeting with a good draft
Sub-team should use Howard Gugel early and often.

The SDT requested that Friday sessions should clearly note if noon is the adjournment time so that members can make travel arrangements accordingly.

The Chair and Vice Chair and the SDT thanked Bill Winters for his excellent hosting and great facilities. Bill offered to host later in the year and will follow up with Joe Bucciero.

The meeting adjourned at 12:15 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT MARCH 9-12, 2010
PHOENIX, ARIZONA

MEETING SUMMARY

I. AGENDA REVIEW, WORKPLAN, UPDATES AND COMMUNICATION PLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 20th meeting noting the Vice Chair Phil Huff would join the meeting on Wednesday morning. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The host Bill Winters, a SDT member, welcomed everyone to the facilities and covered logistics. The Chair reviewed the following meeting objectives:

- Review the revised CSO 706 SDT 2010 Work plan and Convergence Schedule Proposal
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and May 2010 Technical Workshop
- Review, discuss industry comments and identify issues raised to be addressed in revised CIP-002-4
- Review, refine and test consensus on a revised draft CIP 002-4 and Industry Response Document
- Receive progress reports for Security Controls Requirements Sub-Teams
- Develop and Test Sub-Team Security Controls Requirements
- Agree on next steps and assignments

He suggested the Team was at a crossroads in terms of getting some of our product out to the industry and getting beyond conceptual discussions. He noted we need to have complete draft CIP package at the end of our April Meeting for posting for informal comment in early May. He suggested the focus needed to be on getting things done and that once the SDT has agreed then it needed to move forward and not revisit previous discussions.

Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the February 16-19, 2010 SDT session in Austin, Texas.

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.

B. Workplan Schedule Review

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials. Joe Bucierro suggested the SDT might want to review this overnight and take up first thing on Wednesday morning.

On day two, Stu Langton reviewed the SDT schedule sent out yesterday from Scott Mix He noted that this is our 20th meeting over past eighteen months. The SDT has faced four core challenges:

- Over 200 items in 706;
- High visibility issue in the industry and Congress;
- Large team formed in effort to represent points of view of the industry; and
- Two different cultures addressing cyber security-- engineering/production backgrounds and engineering/cyber security backgrounds.

The SDT handled initially the TFEs. In Fall of 2009 the SDT responded to a FERC ninety day order. The SDT experienced a change in leadership and a 25% change in team membership. The SDT has experienced high pressure to shorten the schedule and work more intensely. We added an additional day to most of our 2010 meetings. The SDT has gotten CIP versions 1 and 2 out to industry and broadly accepted and have continued to meet deadlines successfully. The SDT has developed meeting protocols that let members speak and also observers which can be frustrating as we try to afford airtime for everyone. The Team recognizes that we have been asked to address potentially significant changes for the industry. The team has created straw documents which we have been able to respond to a make progress and has developed good quality products. We have used small drafting groups and polling and consensus testing to help group move forward. We get knocked off pace when members feel a the need to offer illustrative examples in order to test concepts that often are tied to particular views or narrow areas of operation. We occasionally get bogged down with disagreements and differences. The key has been to offer improvements not just challenges as we have key deadlines we must meet.

Scott Mix and Joe Bucierro reviewed a schedule Gant chart and Joe's is a matrix for comparison – both are very helpful and provide a game plan that may have to be adapted to respond to additional changes and challenges. Between now and next meeting is important challenge to getting the first draft done. The proposed process involves five key steps:

1. Informal comment period of thirty days for industry to review in May-June, 2010.
2. Formal 45 comment period from July 26 to mid-September.
3. Followed by up to three ballots of ten days each
4. A NERC board decision in December to adopt the new CIP; and
5. Send to FERC by end of December.

Our next meeting is on April 13-16 in Atlanta where we will adopt a draft for industry comment which will then be posted on May 3. We will meet 5/11-14 in Dallas to develop guidance documents and prepare for the Industry workshop the following week in Dallas. On June 8-11 we will review comments on first draft from the industry and the workshop and refine the CIP. On July 13-16 we will finalize and approve documents for posting for formal comment period. This new schedule builds in time for NERC review and work followed by drafting team approval. This schedule will be made available as part of the meeting summary – has already been sent out to the list and includes two webinars as part of communication plan to the industry. The Technical workshop is part of the process for collecting comments as part of informal comment periods. Any comments received during member presentations to key groups should be consistently requesting comments in writing so we do not have to respond to those from memory. The official record needs written comments to capture.

C. Communication Plan

John Lim introduced Carl Dombek the new NERC communications director and asked him for a progress report on the communication plan for the drafting team activities and drafting of the standards. He thanked the Chair for the introduction and noted there would be a broad spectrum of materials and opportunities to consider. They are planning to brief reporters from the various trade dailies bringing them up to speed on purpose of a performance based system. There would need to be more communication to particular groups to make them aware of webinars, perhaps more targeted advisories as opposed to general notices – impressing on them the importance of participating in the process.

SDT Member Comments

- Workshop – any planning for it? Want to do it in mid May – technical workshop to follow the filing in early May to clarify questions and develop better understanding
- Should it be in conjunction with Board of Trustees meeting? Or separate event?
- The Team is proposing a separate event the week of May 17.
- Carl will get with Gerry Adamski to review details and explore new ways of getting participation.
- Where should the workshop venue be? Washington? He suggested it may depend on the number of people attending and he offered to look into that and suggested discussing the specifics offline.

D. Standards Drafting 101

On Wednesday, Howard Gugel, NERC, presented an overview with guidance for the Team on drafting standards and requirements which he and Maureen prepared. He noted the overall move towards performance based standards and described the general process for writing a standard. He suggested starting with the end in mind and FERC's criteria for approval:

- Achieves a specified reliability goal,
- Is applicable to all regions and entities, and
- Considers costs but not at expense of reliability.

It is important for the Team to build consensus at every step. As the Team has experienced first hand this is most difficult to develop at the concepts and assumptions level first, before addressing the drafting of requirements, then measures and compliance element.

SDT Discussion

- What happened to measures – are they going away? Not yet.
- How much leeway does group have to set zero based risk factors? VSLs and VFRs are filed separately, not as part of standard itself.
- Will we have the ability to pick the thresholds? Team will draft those for industry comment, it will be part of the record but not technically part of the ballot, and will be filed separately.
- Industry does not understand that VSLs and VFRs are filed separately.
- In the example rewrite, where does updating the documentation fit? As part of R1 sub-part 3 or as R2?
- Why have update if you are required to have documentation – doesn't that include updating?
- Could we say "continually" document? Then there would have to be an interpretation of "continually"
- The less we leave room for interpretation the better off we will be for purposes of auditing.
- Careful in our requirements that we do not cross the line into the how to do it.
- The audit model we will use seems to assume we are guilty until we can prove our innocence through documentation in the audit process.

II. REVIEW OF REFINEMENTS OF CIP-002-4

A. Initial Review of CIP-002-4

John Lim provided a progress report on the Subteam's work since Austin (*Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton) Rod Hardiman*

(Observer) They met two times last week. Dave Revill has worked on a strawman for us to use and has developed a good set of requirements to work with using criteria posted as a starting point. Jackie has done some more work on those. Rich Kinas is working on the comments – will use the discussion of the team from last meeting.

He reviewed with the Team the following issues the CIP 002 Sub-team has been grappling with:

- **Definitions**
- Definitions of BES cyber system?
- What is meant by "Misuse"? Throw it into the list of things that can cause harm to the system?
- What is compromised if not misused? Just adding to be sure the link between the two is understood by all – 706 said to put misuse into the categorization.
- Do we need a definition of what we are going to protect in order to develop criteria – if we are not going to do that, why don't we create a list of implementation scenarios and work back toward a definition as opposed to tweaking a definition by finding exceptions – work it in the opposite direction – we have a definition that does not work.
- need operations folk to take the lead because they know how it works
- if bright lines need definitions, then figure out the situations it will be applied
- letting impact of generation facility meet the definition because of the impact it has
- **Drafting Language**
- "such as" – in a standard is this inclusive, illustrative or what as a guideline? "Such as" is repetitive and redundant – suggest dropping
- **Control room vs. control center.**
- Control center concept may be going the way of the dinosaur but it is not quite there yet.
- Also control room versus control center – the latter includes the operators – we went to one room.
- Replace center with system which can be in one or multiple places?
- Trying to resolve conflict between geography and functions.
- **Legacy.** How do we deal with "legacy" and the need to move forward and assure the spectrum of needs are protected?
- This is not part of the standard.
- Currently using as an example – but what is in the glossary makes a huge difference on compliance – need to be sure we know and the auditors know what it means and agree on that definition
- **Multiple facilities.** Point to the highlighted additions as added since the last comment period: "multiple locations" and "Real Time"
- "Multiple facilities" and "multiple locations" keeps it from being limited to one site or single generation issue.

- We dropped the location concept in the requirements because it was too easy to get wrapped around the axle.
- Need to be sure we don't get caught with unintended consequences.
- **Control system.** just calling it a control system doesn't cover the need
- do we need this. If we do, should we add "digital control system"?
- it is needed because we have a bright line criteria that addresses this issue
- "binary" not just digital
- Modified guidelines on alarm monitoring to focus on power operations
- Most generator systems have a fire suppression system
- That is fire that impacts operations or restoration functions – that fits operational concept

Added 4.1.10 Distribution Provider (with qualification) –

- Need to clarify what is included in bulk provider definition
- "with BES assets" instead of "qualification" would clarify
- tie to regional reliability organization or its equivalent – existing standards already have appropriate language – see PRC-8 and PRC-10 – to replace language above

5.1

- Take out the parenthetical marks and include the language
- Disclaimer of other group working on defining what is under NERC jurisdiction
- Does "Facility" need to be capitalized? Yes, it is in the NERC Glossary
- is there a separate plan for covering nuclear facilities?
- We have to have an implementation plan for version 3 – still working on developing version 4 for filing at end of December and it must include implementation schedule for everything under NERC jurisdiction

Dave Revill presented the concept of breaking requirements into two components:

1.3 Uniquely identify and document assets

1.4 Identify types of data communication into five technologies: routable, non-routable, dial-up, serial or not networked

- Definitions build on the attachment
- Created matrix using the five categories of communication technology including:
- And assigned high-medium-low as compared with BES impact rating

SDT Discussion

- Why is serial called out specifically? Is it captured by non-routable?
- Do we consider it legacy? It is different from non-routable – actually it is included
- Do we need to call out wireless as a separate family?
- Do not apply the same controls to legacy serial as other non-routable – that is why it is called out
- Mixing topology and protocol – our attempt at creating bright lines may be in trouble –

- I am interested in protecting interconnected systems regardless of the protocols
- Routable at the top because it is the most vulnerable – what are we including in the non-routable?
- Legacy protocols were not point to point, they were multi-drop?
- We will have three sets of controls – there is another dimension for environment – is there a third dimension too?
- Original idea --across the top was if I get to it how much damage can I create and the down the side was how easy is it to reach (connectivity) – not getting into the transport
- We may be digging ourselves deeper into controls – need to keep this separate from the requirements.
- How can you use the cyber system to bring a chuck of the BES down? Industry just wants to know what they have to do – practically talking about someone from the outside patiently, persistently breaking in using routable protocol or a disgruntled insider
- Routable, non-routable and stand alone – we used these categories in Austin/
- We did build consensus on connectivity, and but not on the protocols – broke the connected into routable and dial-up - protocols should be done in the controls
- Propose we are after connectivity – color code the first four lines and discuss what if any break out needs to be included –
- Two categories of connected and not connected?
- Confusing protocols with access – it is the access that makes system vulnerable

After a break, facilitator Stu Langton pointed out the tensions the Team has experienced has been balancing three things: getting the task done on time; doing it well; and building consensus among the team to move forward. He noted in Austin the SDT seemed to have a degree of consensus on three tiers: connectivity/routable/dial-up, non-routable, and not connected. What was discussed before break is a continuance of that discussion. The Team may not need to retest the earlier agreement but simply flesh out what is included in each category. The Team agreed to ask the CIP 002 sub-team in light of the discussion to test where this would or would not work and bring back refinements or alternatives that address questions.

Final SDT Discussion Points on CIP 002 Requirements

- May need a full team approach to refining the requirements?
- Connectivity/routable/dial-up are not all inclusive, dial-up could be included in non-routable too – need various perspectives to test these categories – I am concerned about non-authorized access
- Category should just be "connectivity." But we need to clarify "connectivity"
- Maybe we need to use "accessible" – then define as remotely, local and not accessible
- It is good, we just need to move forward with it by refining it – not locking into these terms and need to refine them using the Sub-team group

- When we have an issue and we don't have a definition we can simply ask each person what the term means to them to try and build a higher degree of understanding

CIP 002 Attachments

John Lim then presented an overview of the approach taken in the attachments.

SDT Discussion

- Is "essential to the reliability of the BES" the same thing as "supporting the reliable operation of the BES system"?
- Suggest changing to "reliable operation of the BES"

Real Time

- "Real Time"? Do we need to clarify?
- Need to be sure we are using terms consistently across NERC standards.
- Is there a catch phrase we can use that captures the concern? Real time operations?
- Within a period of time?
- It means right now up to thirty minutes? Or is it an hour cutoff, the point it must be reported?
- This may have to do with how many megawatts is lost over what period of time that impacts the system
- Within fifteen minutes (or X# of minutes) would cause a disruption of the system – concern is for the condition of the system
- Default Disturbance Recovery Period is fifteen minutes – from the glossary
- Allowed thirty minutes to recover
- This is an example of two different standards we are drawing upon for two different requirements – can NERC help identify applicable comparable standards?
- Note that the thresholds for reporting something and time for correcting it may be different for the same standard.
- Looking at other standards from other teams is a novel concept for most drafting teams.
- 30 minutes for IROLs in three different requirements – supports using that time frame
- Concept of time horizons of reporting and correcting are not germane to protecting the BES.
- "Real time" captures it even if it is a fuzzy term.
- Does this mean you have to prove to an auditor that you can anticipate all the possibilities?
- IROLs are part of the reliability coordinators role.
- Part of developing standards is the need for setting time horizons for severity of violations.
- Real time is action required within one hour to prevent further damage to the BES – comes from guidance document for establishing time horizons.

- Putting in specific times may not be needed here – "real time" for purposes of auditing may be too wishy-washy.
- Should we test with a vote and move on?
- Leave as is and then when we write the requirement say "real time operations" that then refers back to the NERC guidance.
- Do we need to specifically reference here the real time operations in the requirement?
- Put in parenthesis since it is not in the requirement but in the guidance
- An ad hoc team was asked to address: including Howard Gugel, Doug Johnson, Dave Revill and John V. Boxtel.
- Issue may not be not real time operations but the definition of immediate impact

Audits, Standards and Guidance

- All this is part of the standard as an attachment? Or is this only guidance?
- If the former then I need to be prepared to address the sixty or so bullets as possible items for audits? I have to prove everything in the attachment if part of the standard.
- Thought we were moving it to guidance
- Have we switched the numbers of attachment one and attachment two from the last meeting? Yes.
- We have two attachments even though at the last meeting we agree to meld into one attachment and moving much of the old two into guidance?
- Keep the opening paragraph under dynamic response and move the bullets to guidance?
- That may be worse.
- But we have to define this somewhere.
- We are here to protect reliable bulk power not simply to make compliance clear.
- We have to identify critical functions and how we will protect those functions.

Functions.

- Functions ended up in the definitions then pulled back out as being too broad for the definitions and were put back into the attachment
- Functions have never been incorporated into what we are trying to do – our approach to reliability is to look at how much a system impacts the grid – concerned we are arguing about the same concepts as six months ago
- Functions for reliability must come first – the level of controls will come from table 1

Disturbance to the BES.

- Are we really talking about anything that can cause a Disturbance to the system? Reviewed the definition of "Disturbance" – only functions of significance are those that can cause a "Disturbance to the BES"
- But that does not include situational awareness
- Can we use an existing NERC term and build on it?
- Do we want to leave vague terms and leave it up to auditor for interpretation or drill down into the details?

- I would like to use existing terms like "Disturbance"
- Can we throw ideas out about how to address the concept of combining into one attachment and the rest to guidance?
- We have already posted a version of comments and changing based on comments not trying to rewrite the standard completely –
- There was no comment about removing functions from attachment – there were comments about removing examples – if repost radically different standard we will get a whole new set of comments.
- We do have the ability in this new CIP standards process to offer changes.
- The primary issues are the scope to be addressed – hopefully building a significant yes around this table will help build a significant yes in the industry –
- Can we spend time on BES cyber system scoping? What is the context of effect and the context of time and connectivity – I like drawing on existing definitions if possible.
- Disturbance plus: for purpose of defining the scope of applicability of SIP standards, the functions of relevance are only those which could cause a Disturbance to the BES, restrict control and operation of the BES, or affect situation awareness of the BES
- Can we just define a list of systems that do the things we want to cover such as for situational awareness and determine a list of what to protect?
- Concerned that we are not building on success but only re-discussing the same issues – the industry wants to clarity
- Anything in NIST that can be used as a starting point?
- Nobody has come up with anything that should not be in attachment 2 – IT does not know what is vital for protecting the reliability of the BES – bulk produces determine what is essential and cyber can help figure out how to protect.
- What we have here is an effort to provide clarity – this is the stuff to protect
- Lets take this and make clearer what we are trying to protect
- Situational awareness may take more effort since it is a little squishy – but much of the rest is concrete enough to work with
- Those in the control world can look at the list and see if it can be made more concrete – others can work on the connectivity box – then see if we can jell them together
- Defer where it goes until after we set what we need
- Will we end up with anything different than the list we already have?
- We are describing things by functions
- List essential functions and leave it to entity to determine which meet that and offer guidance on what you think – serves as an interim step
- I like idea of moving sub bullets out to guidance, leave in functions with a matrix
- That puts focus on each group creating the list they need then cross reference to the IT guys to help figure out how to protect it

Addressing Industry Comments.

- Need to go back and read some of the comments that were offered. What are they telling us about Attachment 2?
- Regarding Attachment 1 and 2 – industry wanted more specifics of what is to be protected so we provided the attachments – now they comment back that they don't like specifics – industry will not be happy because it will have to spend money and resources to address it
- What does the statement above mean to an auditor?
- Jay pulled out and read from a comment a draft definition that might address the issue
- The bullets added clarity while the general definition offered to cover the breadth of situations.
- We have not discussed the suggestions for refining offered in the comments – those could be part of a brainstorming effort to addressing the question.
- If we take into account all the comments offered we will end up with the standard you have now because industry doesn't want to change because it will cost them resources.
- We cannot make radical changes to the documents we have posted and expect to build consensus or broad base of support.
- Looking for members to pull forward key concepts from the comments for group consideration
- We did not do justice to the comments by only reviewing summaries and only considering them in small groups or just asking members to read them on their own.

B. CIP 002-4 "Parking Lot" Issues

During the course of the first day's discussion the following issues were noted, but not resolved, for sub-teams to return to:

1. Multiple Locations – concerns raised re: rationale
2. Cyber Security Incident Definition
3. Distribution Provider – concerns regarding inclusion
4. Presence of R1 and R2 could present double jeopardy concerns
5. Define "change in BES" (R3) Long term? Etc.
6. How does one audit R3? Is there an implied requirement of maintaining a list of changes?
7. Clarify the link between Attachment 1 (R1) and Attachment 2 (R2) and where to capture the link (Guidance? Standards?)
8. Distribution (used as stabilizing load during restoration) for Blackstart?
9. Standard in development of High impact system – reference: Project 2009-09
10. My comment agreed was that 1.11 effectively includes all BES Facilities greater than 300kV. An option might be to delete 1.11 and include something like the following in every other item (using 1.1 as an example):

11. APP #2: 1.11 effectively includes all BES Facilities greater than 300kV. An option might be to delete 1.11 and include something like the following in every other item (using 1.1 as an example):
12. APP #2: 1.1: Generation Facilities, and their associated Protection Systems, singularly or in combination...
13. BES Cyber System vs. Cyber System?
14. John Ciufo – Standard in Development – High impact system – reference Project 2009-07

Based on a review of the parking lot issues, the Team agreed to the following drafting assignments:

1. **Control System** – Produce a list of examples – Rich Kinas

On Day 2 Rich presented a draft list of examples for control systems.

SDT Discussion

- Only to the low side? This is what the industry does now – what they are thinking – we need to fit in or make clear what we are talking about to avoid confusing the industry
- Some of the industry does go further
- This is a means or tool to the end of clarifying intent
- May be part of guidance document
- May want to include other ways industry is addressing – these are not exhaustive, only initial thoughts

2. **Matrix Group – "connected/not connected**" – Jon S., Jackie, Bill, Jay, Rich, Patricio (John V. Boxtel)

Jon Stanford provided an overview of the points of agreement after the group reviewed the list of points from discussion yesterday in its discussion the night before.

- Bright line was a good idea and effort but may not work after testing several examples. It could be counter productive
- In CIP 002 it is important to get object or target of protection.
- Applying connectivity can become very complicated.
- Entity has to decide what is a BES – cannot cut systems up into small pieces – so we all should "get over it."
- The low baseline needs to be those controls/requirements that provide the highest value to mitigate risk.
- We shouldn't let "audit fears" limit our ability to develop meaningful standards, instead let auditing adapt to the new standards.

- We shouldn't' be afraid of if/then/else application of some controls/requirements as appropriate.
- The team had consensus that control work should move forward in parallel to the 002 work – i.e. we should develop catalogue in tandem not in sequence.
- The team agreed there needs to be more guidance to sub teams
- This will capitalize on work already done by sub teams in developing controls.

SDT Discussion

- Does this apply to controls not requirements? We cannot put "if then" in the requirements.
- Still to be determined in the language to be developed. Most of this discussion is about controls and writing requirements – apply focus on practicality, lot of industry comment referenced routable protocols.
- Putting "if/then/else" introductory language before the "shall" phrase may be workable and has precedent in other standards.
- Auditors will audit to what the requirement says – need to capture words in the requirement that we want them to audit to – crisp accurate language so industry knows what will be audited and auditors will know what to audit too.
- Sub group work needs to use consistent language across the standards – need a common language whether it is h-m-l or something else
- Confident if the right things coming out of 002 then we can set the right "bright lines"
- 002 is an identification exercise – current standards do not allow you to take into account how assets are deployed – this new approach does if controls written properly.
- 002 will identify the important things to protect and the assets related to those regardless of type of connection. We understand that technology will change and the standards will need to incorporate and adjust to those changes over time.
- Does this take away the connectivity piece of the evaluation? Closer to what we had before? Need to decide and start drafting controls.
- Can still include routable protocols in 002 if it would provide the best industry response and compliance if that is the way the industry thinks.
- Yes, we need to put stake in the ground –but it is not either or – can we address connectivity in the controls? Need more discussion of how many controls will be in the "low", may be a small number
- NRC guideline effort struggles with the same issue – they have an appendix B "mandatory" controls and appendix A technical security controls with an exceptions process – you would have to show auditor you do not have "connectivity"
- Good concept but a few things bother me. "Don't be afraid of audits? Not afraid, but not sure how to accomplish
- Take the language "with a grain of salt"– starting the discussion, not meant to be inflammatory.

- What I want to happen is that anything out of 002 should address making the system more secure – don't care if high or low but whether or not adequate protection is provided certain controls
- Lot more common ground than at first appears – want to consider impact on the BES, the connectivity, and how we apply controls – trying to get the same end of controls appropriate for the environment
- Common on the end result – still struggling how it is understood by the industry which sees their world changing.
- Does it make more sense to come up with complete list in 002? If industry concerned about increasing scope to non-routable you need to explain the intent to them – also addresses Congressional concern past standards did not address everything – explain to industry that not everything is high and that listing into low where appropriate helps focus efforts on the important things.
- Problem with government NIST system is that too much is low with little more in medium and little more in high.
- Too many are avoiding updates by using the non-routable as an out.
- Federal low is not there because of IP – the low is too high – and the enhancements in the high category are significant to the most focused items. This may not be good optics, but we need to educate the industry and congress on the issue.
- Entities are not moving forward and are pulling routable protocols out to take advantage of non-routable exceptions and may be impacting protection of the system.
- Setting the routable protocol as the bright line can thus be counter productive to protecting the system.
- NIST is modeled for a different system than the private sector industry - also CIPs are not written for special situations but for the majority of the industry.
- Non-routable is not a loophole and may be reducing exposure and improving security if can remove the routable protocol.
- The NIST is offered to show why it will not work and why we are offering a more tailored approach applicable to the industry.
- All still getting to the same level of security and controls to apply – the end of 002 is not a list of h-m-l impacts but identifying the appropriate level of controls to apply.
- We are not advocating applying 853 – just illustrating the approach.
- Also trying to address unintended consequences and trying to avoid spending money on things that will not improve security of the system.
- Each of us heads off in different directions to fit our world –
- Let the 002 sub-team do their work and let the other teams begin developing the base line rather than the high first, develop the universe then look at how to apply connectivity.
- This is an example of how this team struggles to make decisions without seeing details – can we draft security controls without looking at connectivity?
- Two main concerns – is non-routable in 002, if so, are they now addressed?
- If artificially in low or high will have to spend money unnecessarily to protect. We may need to figure out what is in the h-m-l first.

- Everything starts out as at least low – should connectivity be addressed in the standard or in the controls?
- I think we do have a non-applicable category too – a bottom to the standard is set by applying the real time function
- Industry is spooked about making an inventory of all assets – we are proposing an inventory of those functions impacting the reliability of the BES – that is good business practice

3. **Real Time Operation/Cyber System affecting "immediate impact"** – Dave Revill, Howard Gugel, Doug Johnson, (Jon Van Boxtel)

Howard Gugel presented the group's report making the following points:

- The group suggested that functions of relevance are those functions essential to reliability of the BES. If it affect situational awareness does it exclude anything?
- Read the definition of situational awareness. A unit, a station? That is the way it is defined if can affect reliability of the BES.
- Entities currently know what those are.
- Information that can cause a bad decision that impacts the BES reliability.

SDT Discussion

- "Restrict" control of operations? Need to clarify the term – affect or constrain?
- Every entity has a different situation they will need to be aware of – depends on who you are as to the level of awareness
- Is this a good subject for a glossary term? "situational awareness"?
- This is an effort to take the attachment one from yesterday and try to address situational awareness
- Need to make sure that if in the standard we have supporting language in guidance
- Situational awareness is organizational behavior but not necessarily BES function
- Can apply to many things beyond just functions
- The term is a major cause of problems in Florida and the 2004 blackout
- Proposed modification – display of data that could affect function – "which could adversely affect the performance of a reliability function" –
- Trying to address where "monkeyed" with
- Everything there could adversely affect yet none of them are designed to cause adverse affects

4. **Attachment 2** – guidance, matrix – Rich Kinas and John Lim.

On day 2 Rich presented a draft guidance document. He noted:

- Dynamic response example – spinning reserves might be GOP function;
- Created table to help entities figure out which functions to address.

SDT Discussion

- Is this the same as Real Time operations?

- This could be part of that group but not the intention.
- Under suggested improvements – collapse some of the categories?
- Specific requirements for TO and TOP – different roles and different companies may be addressing each
- Flushing this out should not take too much time but be sure architecturally sound
- One thing under current CIP we had to assign assets to individual functions – be sure we do not become overly proscriptive
- What do we need to document for registered entities and ties to others for assignment of functions?

C. CIP-002 Guidance

In conclusion the Chair and Vice Chair reminded members that the Team has a very tight time frame to get our work done and they need to emphasize and trust the small group work and giving them time to get products ready and test with hard breaks for moving forward. The Team recognizes that 22 members cannot collectively write the standards within the time limits

The Team tested the level of support for the following guidance to the CIP 002 sub-team:

3. **Redraft CIP-002 to remove the connectivity options and handle them in the controls**
   Y= 15 N = 5

4. **Keep cip-002 as drafted yesterday and let cip-002 sub-team handle modifications to the matrix (Austin)**
   Y= 4 N= 16

The Team acknowledged they may need to revisit if in developing controls we find we cannot address the connectivity issue.

D. CIP 002 Drafting Group Update Report

John Lim reported on Thursday the Sub-Team's efforts:

- 002 completed most of the work on the requirements.
- Attachment 1 is definitions of the functions.
- Working on attachment 2 applying functions- working on that tonight.

He suggested that on Friday the SDT should concentrate on the standard document itself.

E. CIP-002-4 Review and Consensus Testing

On Friday, John Lim presented the revisions to CIP 002. He asked the SDT to focus on the content and intent of the draft and not to engage in word-smithing noting that there were extensive and challenging discussions among the Sub-team over the past few days. Focus on content and intent of document.

- Will send to Howard for editing and review.
- New work on Attachment 2- levels.
- The Sub-team removed definitions of functions for reliability of BES and moved them to Attachment 1.

1. Definitions

- "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 if rendered unavailable, degraded, compromised, or misused could cause a Disturbance to the BES, restrict control and operation of the BES, or affect situational awareness of the BES."

SDT Comments

- Do we have to start with BES before cyber system?
- Definitions- should be stand alone. Context comes in the requirements.
- Clarify the purpose of standard and this definition?
- Will this be added to glossary? Control center length?
- c. Real time capitalized? b. no capitalized. Proposing to go in the NERC glossary.
- Only "Real-time" in glossary. "Present time as opposed to future time." Lower case "real time" in document.
- Would it affect definition to leave real time out?
- Might confused.
- Real space time. Some of operations- not now but 20 minute horizon.
- SM: did agree on the qualification "alarm monitoring and processing"
- Add to d. <u>specific to operation and restoration functions.</u>
- BW: is it better to use now "real time" as a qualifier.
- HG: glossary definition doesn't capture. Use lower case.
- JL will do a real time edit.
- RK: Quick search of other NERC standards.
- JC: definition developed.
- AL: why was multiple locations in the document?
- Retiring 3 terms.
- Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:
- Critical Assets
- Critical Cyber Assets

- Cyber Assets

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-4

3. Purpose: To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES for the application of cyber security requirements commensurate with the adverse impact that loss or compromise of those BES Cyber Systems could have on the reliability of the BES.

SDT Comments on changes?

- One issue we will have to do with it. Removing "critical cyber assets" and "electronic security perimeter." Will have to add definition for that term.

Distribution Provider

- Reference to PRC 5- distribution providing owns a transmission- this is a transmission Protection System.
- Cover in guidance document. 6-7 PRC standards talking about special protection systems, etc.
- Looked at all this. Need to put in there. Look at registration text, it includes all that information. Those standards deal with under voltage etc. It is covered by a functional definition.
- Provides for changes in regulations.
- The Sub-team didn't agree with this one. Put in the parking lot.

B. Requirements

R1. In order to identify appropriate BES Cyber Systems for the application of security requirements or controls, each Responsible Entity shall uniquely identify and document all BES Cyber Systems which execute or enable functions defined in *CIP-002 – 4 Attachment I – Functions Essential to the Reliable Operation of the BES*.

R2. In order to categorize the BES Cyber Systems identified in R1 to apply Cyber Security requirements or controls commensurate with the potential impact on the BES, each Responsible Entity shall categorize or re-categorize each BES Cyber System according to the criteria contained in *CIP-002-4 Attachment II – Impact Categorization of BES Cyber Systems.*

2.1. The Responsible Entity shall review its categorized list of BES Cyber Systems, as a result of any change in the electric system that it owns or operates that affects the categorization of the BES Cyber System, and update within 45 days of the completion of the change.

Controls standards will specify applicability to the BES Cyber Systems categorized in this standard.

SDT Discussion

- States the reliability benefit in the requirement.
- Can't have requirement that starts in the middle? Need BES before BES cyber.
- Clean up wording on requirements.
- Need BES- agree JV- Not clear these 2 requirements what have to put in BES.
- Is 2.1 is a separate requirement?
- Add "In order to maintain and keep current the list…."
- Change 45 days to 30 days to be consistent with FERC directions.
- Why 2 requirements? Is it possible identify and characterize as 1? Looks like a step to an end result.
- R1- identify all BES.
- R1- to id cyber systems based on your BES. It would be more confusing to combine.
- Howard Gugel noted that you could combine as 1 requirement or leave as 2 separate.
- Is there an issue of double jeopardy? Forgot to include one and not categorized correctly? Look to defining your VSLs.
- 2 separate lists because of 2 requirement? If expect 1 list then 1 requirement. If 2 lists then double jeopardy question may be raised.
- Change in R3- "change in the electric system"?
- The Sub-Team removed BES cyber systems from here. Assumed will be covered in Change Management group. Couldn't find mechanism for update.
- Howard Gugel suggested striking "that affects the categorization of the BES" instead. Anytime you add anything new to your BES cyber system you have to update.
- R1- likes the unique identification and document vs. make a list. Entities are using something similar to a list? R3 updating "your documentation"
- Suggest edit: ~~electric system~~ BES
- Pick up commissioning activities, changes in BES cyber system in change management. Do an annual review and update and capture changes in system 1 time a year and that will capture this.
- Need to define "changing electric system"- what does this mean?
- "Commissioning new assets"
- Don't like "any" change. What does this mean. Needs a qualifier. Updating the documentation specified to R1? Keep update the list.
- R2.1 separate? Wasn't under posted version.
- Any change? Long-term change? E.g. bringing new line on?
- Howard Gugel suggested: "When any BES ~~element~~ facilities is added to or retired from the BES that it owns or operates."
- What about "modify"?
- R3- refer to R1 documentation
- Simplify to going back to R1. Not separate

- Requirement is for reliability and not documentation.
- 45 days? FERC said 30 days. Will need justification.
- How do you audit R3?

Parking Lot
- "Multiple locations" definition- concerns whether it is needed?
- "Cyber security definition"?
- Distribution provider?
- R1-3. If 2 requirements

Data Retention
- Less than compliance time frame? Maintain as 1 year. "Keep for the compliance audit period, 3-6 years depending on what kind of entity." Global issue for every standard. SDT has to figure out whether we stick with it.
- NERC should do this.
- Full year or …… Clean up to make consistent.

Violation Severity Levels.
- Team used NERC guidelines for VSLs to make consistent.
- "Or" is for 2.1

SDT Comments
- VRFs? They will be put in. Both will be high
- First line- in terms of audit? Look at your diagrams and go through steps.
- Open to suggestions.
- Don't audit that item. Combine process.
- Comes out in an investigation and 3 level process
- The auditor looks at what you present and drafts a "potential violation". Audit process stops and goes to investigations and further analysis. Not an audit function triggering thresholds.
- That's why we left this as is.

CIP-002-4 Attachment I
Functions Essential to Reliable Operation of the Bulk Electric System

The following operating functions are defined to be Essential to Reliable Operation of the Bulk Electric System (BES):
- Dynamic response
- Balancing Load and Generation
- Controlling Frequency (real power)
- Controlling Voltage (reactive power)
- Managing Constraints
- Control & Operation
- Restoration of BES

- Situational awareness
- Inter-Entity coordination and communication

For purposes of defining the scope of applicability of CIP Standards, the functions of relevance are only those that affect real-time operation of the BES. Further qualification as to what constitutes Functions Essential to Reliable Operation of the BES can be found below.

- Will place and develop it in the guidance documents.
- Make sure consistent with "real-time" definitions and any other changes in definitions discussed.
- Actively performed functions not reactions.
- Had this under dynamic response.

Attachment II

John Lim reviewed the development of Attachment II which Jackie Collett help to develop.

1. High Impact Rating (H)

BES Cyber Systems that would immediately affect real-time operations for:

1.1. Generation Facilities, singularly or in combination, with aggregate higher of the most current and prior to the most current rated net demonstrated capability (MOD-024 and MOD-025) of 2,000 MVA or more.

1.2. Generation Facilities, singularly or in combination, whose aggregate rated net demonstrated capability, as defined in part 1.1 above, exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group.

1.3. Generation Facilities that are pre-designated as Reliability "must run" assigned units that have Wide Area reliability impacts.

1.4. Generation Facilities designated as blackstart resources in the regional blackstart capability plan.

1.5. Transmission Facilities operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 KV or higher in other Interconnections. (3 or more …)

1.6. Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005.

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

1.8. Transmission Facilities that if destroyed, degraded or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated Net Demonstrated Capability (MOD-024-1) of 2,000 MVA (?? TOO LOW ??) or more

1.9. Transmission Facilities identified as essential to meeting (verify wording) Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for Nuclear facilities.
1.10. Transmission Facilities that, if destroyed, degraded or otherwise rendered unavailable, would result in voltage collapse, electric system collapse due to frequency related instability, or complete operational failure of the Transmission system or separation or Cascading outages. (linked to IROL criteria - wording)
1.11. Protection Systems for BES Facilities operating at 300 kV and above in the Eastern and Western Interconnections, or operating at 200 kV and above in other Interconnections. (Hardiman: establish 300 kV baseline)
1.12. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements and that have wide-area impact.
1.13. BES Elements that perform automatic aggregate load shedding of 300 MW or more.
1.14. Primary Control Centers and any backup Control Centers performing Reliability Coordinator functions.
1.15. Primary Control Centers and any backup Control Centers performing Balancing Authority functions of Transmission Facilities or generation Facilities, singularly or in combination, of 2,000 MVA or more.
1.16. Primary Control Centers and any backup Control Centers Transmission Operator functions that remotely control 2 or more 300 kV or higher Transmission substations or switching stations.

SDT Comments

- Lead in sentence. Is the cart is before the horse-- the 1.1 piece. Say something about BES systems first.
- The Sub-Team removed all reference to systems. Now referred to "facility elements" from the NERC glossary.
- Referring to generator rating standards? MOD 24 and 25? No more "opt out" – rationale is reference to MOD 24 and 25, engineering studies already authorized. No good reason to have "authorized engineering study"
- Where do we address 2000 number? Went through event analysis category- Category 3. Talked solely about generation and supply.
- 1.1."Nameplate generation rating"- use something we already have- "current rated net demonstrated capability.
- 1.2- time limit-
- How do we link this to defining the BES functions? Where is the correlation? BES functions called out in R1- initial scoping. This is R2 piece that links- then you go through this criteria.
- Are all functions equally weighted? No weighting, just a scoping.
- The Sub-Team tried to take out anything that isn't essential to reliability.

- Operations manager of reliability center- "immediately affect real time operation" - will this place everything low?
- "Facilities"- h/m/l baskets. 3rd basket is things that are not facilities? Have to first determine what "facilities you have."
- BES is a defined term. Says that regions will define. "Generally operated ….."
- Defined by the IRO- have to go by this.
- What is the connection between Attachment 1 and 2? Functions then rating. Need to make this clearer.

1.5 Must run units.
1.6 Blackstart Capability plan.

SDT Comments

- Regional blackstart- includes distribution- used as a stabilizing load during restoration-- include in a guidance document.
- Does this bring into High lots of things not having to deal with transmission?
- Distribution SKADA systems? All? Some?
- This should be a "parking lot" issue.

1.7 "Transmission facilities"- 3 or more connected to station. Add back in.

SDT Comments

- Is 300 KV too low? This came from another document. Few if any industry comments about voltage level. People haven't thought through the impacts on the industry.
- Didn't focus on voltage. Commented on 3 lines being too low. More understanding 300 for a high? This will bring in a lot of locations and equipment.
- Optics- raise to 500 KV portions of interconnection that don't have any. Keep voltage level but adjust the number of lines.
- Consider throughput megawatt? Original draft- inappropriate measure for transmission? Use voltage.

1.8 Number of comments- clarified by referring to EOP -5
1.9 IROLs reference. Decided to stick only with IROLs.
1.10 Rewording of what it was before.

SDT Comments

- Linkage with 1.1? 1.8 is more far reaching than 1.1. 2000 MVA is too low. 2000 MVA may be good at the medium level?

1.11 "Essential to meeting"= (verify this wording)
1.12 Transmission facilities.

SDT Comments

- Without engineering analysis can you do this?
- Link to IRL- reference and work on wording.

1.13 Protection systems- now high- lot of discussion

- Comes from other standard

SDT Comments

- Part of 1.5? Every 300 KV has a protection system. Every 345 KV device that has protection device, 1.11 equivalent to 1.5.
- Inconsistencies related to actual impacts?
- SM: John Sykes- Systems Control committee- determining high impact systems. Standard isn't finished. Reference that when ready?
- Simplify and lump all together in terms of 300 KV?

1.14 Special Protection systems (SPS)

SDT Comments

- Use 1.3- language- "that have Wide Area reliability impacts."

SDT Comments

- Consider adding language: "If the BES operates at N-1 or higher, should field asset criteria indicate an inherently lower impact category than control centers.
- Aimed at T/G/CC- when have requirements that apply to G but not T. Met the criteria.

Medium

2. Medium Impact Rating (M)
   - 2.1. Generation Facilities, singularly or in combination, with aggregate higher of the most current and prior to most current rated net demonstrated capability (MOD-024 and MOD-025) of 1000 MVA or more not included in Section1 above.
   - 2.2. Generation Facilities that are pre-designated as Reliability "must run" assigned units that have local area reliability impacts.
   - 2.3. Transmission Facilities operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not included in Section 1. (include 3 transmission lines)
   - 2.4. Transmission Facilities that if destroyed, degraded or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated Net Demonstrated Capability (MOD-024-1) of 1,000 MVA (?? TOO LOW ??) or more, not included in Section 1.
   - 2.5. Protection Systems for BES Facilities operating at 200 kV and above in the Eastern and Western Interconnections, not included in Section 1, or operating at 100 kV and above in other Interconnections, not included in Section 1.
   - 2.6. Primary Control Centers and any backup Control Centers Transmission Operator functions that remotely control 2 or more 200 kV or higher Transmission substations or switching stations not included in Section 1. (generation control centers ??)

SDT Comments

- Write cyber security requirements apply to H/M/L – is there enough to make a difference in cyber security controls? "Decimal dust" difference.
- Is there a difference between moderate and low? If you draw line at moderate or at high?
- SDT members should go back home, next week a count of facilities that would meet the current criteria. How many are we talking about any of these buckets?
- Control generation? 2.6- generation control center?
- 2.6 would catch all transmission owners? Anything above 200 KV.
- Captures registration errors?
- Definition of BES Cyber Control System? Whether we do cyber system alone. Cyber system definition- to separate from BES cyber system.
- Always refer to BES cyber system.

3. Low Impact Rating (L)
   All other BES Cyber Systems on the list not mapped to Section 1 High BES Impact or Section 2 Medium BES Impact.

SDT Comments

- BES subsystems should be BES cyber systems

III. SECURITY CONTROLS REQUIREMENTS (CIP 003-009) REVIEW

A. Initial Sub-Team Progress Reports

On Wednesday the Sub-teams presented brief status reports before breaking into sub-team meetings. The chair and vice chair suggested the sub-teams should initially focus on setting the "low" for purposes of controls. Need to set a common agreement on where the low water mark is – wrestle with high and medium later.

SDT Discussion

- Do we have the buckets of lists for consideration?
- Support the idea of starting with the lows. This could be a good process and help sub-teams understand what they are addressing.
- Need to bring different perspectives to the task of identifying and establishing a common low water mark

- **Governance Sub-team.** Jon Stanford noted that the Governance Sub-team has nothing new to report but that they do have the list to review for consideration of the low water marks.

- **Access Control & Audits Sub-team**. Sharon Edwards reported on the Access Control & Audits Sub-team noting they have identified CIP requirements we are looking at as compared to DHS – some of the latter did not have a corresponding CIP requirement. They have also constructed template from individual worksheets including constructing requirement language to address missing DHS items. They have not yet distinguished h-m-l and did not yet review FERC order to be sure issues addressed. She suggested a need to coordinate some of the DHS items with the work of the other sub teams. They also added a column not in the template for all the groups – "CIP version 3 language."

- **Recovery and Response Sub-team** – Scott Rosenberger noted they had not made a complete review of DHS.

- **Personnel and Physical Security**
- Doug – have a spreadsheet and prepared down through h-m-l and initial pass through CIP, review as group today before cut and paste into the template

- **Change Management, System Lifecycle and Information Management.** Phil Huff noted they had gone through CIP language and added DHS security controls where appropriate and they determined initial applicability. They will be making an initial h-m-l determination for the controls. Putting in objectives now in at the time of writing the requirement may help in interpreting the intent later.

- **Operations Security.** Jay Cribb reported his sub-team had taken one stab at objectives but not h/m/l.

The facilitators noted the teams are at different levels of development – may want to test with those teams that are ready.

B. Sub-Team Reports on March 11, 2010

Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson(Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin

The Sub-Team report was delivered by Doug Johnson.

Personnel
Awareness programs

- Policy? Expecting the Governance group to address.
- "establish, document, implement and maintain"? continue to use this with other Team? CIP Version 3- not removing it.
- "Information protection program," develop an incidence response procedures? As long as you can test it and demonstrate it works.
- Looking at a low level. If you have BES cyber systems, you will have an awareness program.
- Inter-connective of operations control – 706

Training

- "at a minimum" vs. "appropriate to personnel roles and responsibilities"

Personnel Risk Assessment

- 706 guidance- special circumstance that allow an exception to requirement for training prior to allowing access.
- Program has to specify the exceptional circumstance-
- Anyone with access to BES cyber system. Is that everyone down to the low levels?
- Any baseline opinion- Lows? Electronic or physical.
- Degrees?- cleaning crew.
- Lows?
- If you have physical access to a low impact BES cyber system, do you have to have a personnel risk assessment?
- If there is a requirement for physical access, have to have controls in place.
- Need to be tracking to have an issue.
- We should be thinking about this in terms of risk. Authorized users, maintainers of BES cyber systems. 2 communities here. Opportunity to split and get to risk.

- Interpretation- acceptable alternatives are…… E.g. social security number for verify identity.
- Identification issued by federal, state or provincial agencies.
- Don't worry about the methodology- worry about the right people and provide the level of granularity.
- NERC Interpretation- identify verification, risk assessment. Try to make clear. E.g. Janitor in control room-

Physical

- Physical Security Perimeter- revise current Glossary definition.
- New definition proposed. Limit it to being just a "border" and control access to border. You will have to define where it is and later what's in there.
- Only if you have a defined physical security perimeter.
- "All equipment comprising a BES cyber system shall reside within a defined PSP."

SDT Comments

- "within one or more PSPs?"
- That is better. Tweak to deal with the Hoover dam issue.
- E.g. a "laser field"-
- Leave the definition at a higher level.

Physical Security Plan

- Senior manager approval in new version?

SDT Comments

- 706 requires this.
- "Authorization" = standard language? Current doesn't say who authorized or designated.
- Addressing cross references- highlighting to coming back to. Flagging for now.
- In governance- senior management- remove subordinate references to SM? Talk about what they need to do not how. Let the program set that out.

Physical Access Control

- Controls- this will go off to a guidance document.

Monitoring Physical Access

- Blue will be the "how". Saying you will have it. Go to guidance document for the how.

Logging

- Same

Visitor Control Program

- Same.

Maintenance and Testing

- Need to get with Sub-team defining the perimeters to determine physical control. Keep that in this?
- Don't put in standards in terms of how to protect.

Protection of Electronic Access Control Systems

- Should move these out of standard.
- Are these part of the BES cyber system itself? Protect the system performing the functions.
- The Team needs more discussion- what is a BES cyber system, how to draw the line around these?

SDT Comments

- SM: 706 review? Partial. More discussion.
- Training the trainers- quality and consistency among them. Part of directive.
- Web based training- no instructors.

Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl,

Scott Rosenberger reported on the Sub-team's progress noting they made it through DHS requirements.

Response

- Draft 5 requirements: incidence response you do partially in high and low.
- All will have a plan. Identify actions; roles and responsibilities, reporting, reviewing your plan annually.
- R2: additional for high impacts- review plans based on changes. Communicating updates; Testing response plans annually.

SDT Comments

- Does this requirement apply to all cyber systems?
- This only applies to high. The plans dealing with high impact- add language: "for their high impact basis"

- CIP 008 Cyber Security Incidence- still to figure out.
- CIP 008- R3- document retention- all
- CIP 008 R4 (high) and R5 (low)

SDT Comments

- Annual= once every 12 months?
- BES Cyber assets? Not a new term. BES Cyber Systems-
- In Personnel training requirement- address once every 12 months.

Recovery Plans CIP 009

- If low don't have to have a recovery plan. Only applies to high.
- R2 Recovery Plan Training
- R3 Recover Plan Testing.

SDT Comments

- Place this into table/format with changes? Yes.
- Worked with Scott/Howard re formatting.

- Important to see whole standard together. Everyone had changes.
- Valuable effort- to see how this will sort out. E.g. 1 section for every one. Then some for high, low.
- Didn't see a control- Security of the back up configuration? Current standards- not part of system. Could store elsewhere unprotected? Is this a potential attack vector? 1.3 of CIP 009- back up storage and protection will address.
- Requirement to restore whole system and make sure it still functions (no corruption, passwords, etc.). Restore to as it was.
- Need to think through whether you want the same VRF for everything in requirement. Put in 1 requirement. If you want VRF differentiated, you will need to split the requirement out. E.g. if you have high, these things need to added to you apply.
- Where do you store backups?- Falls in information protection.
- Connectivity concept? Didn't include at all. Where to add? Whether connected or not still need to be restored.

DHS New Requirements

- Control centers- back ups- alternative locations. Didn't seem to apply to generation, transmission.

Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*

Sharon Edwards reported on the Sub-team's work as follows:

Update

- Created the proposed requirements for all assigned CIP requirements that have a corresponding DHS control
- Reviewed the proposed requirements corresponding to CIP and identified which controls should apply at the H, M & L for (C, G. T)
- Created proposed requirements (where applicable) for additional DHS controls which do not have a corresponding CIP requirement
- We have not yet reviewed those to determine if they should apply at the high, medium or low level

Future Tasks

- Group will attempt to gather all the account management requirements currently found throughout CIP 005, CIP 007 and CIP 004 into one place
- Ensure the following are done for each assigned proposed requirement:
  - Identify FERC Order 706 paragraphs & how they are resolved
  - Ensure Objective has been documented
  - Ensure CIP changes have been documented

- Group has decided to determine applicable password thresholds utilizing the NIST password tables and determine what the High, Medium, and Low targets should be – Frank
- Review for impacts of Connectivity on the proposed requirements – Team assignment

Points of Coordination

- Coordinate with Ops Security re. log monitoring and log monitoring for failed log ins based on passwords. – Sharon

SDT Questions and Comments

- Access to Information- Talked to Phil Huff's team- they handle access to information.

Account Management

- High levels- applies at high and medium levels. May be time parameters may change at medium levels. E.g. revocation of access within 6 months., Not a compliance area.
- All will apply at the high, much applies at medium with time parameters relaxed, majority will not apply at the
- Revoke "remote" requirements? 2.15.3- R4- Doesn't meet requirements of 706- revoke 'immediately'? 24 hours too long? Especially for highs.
- High and low- look at total list of being low before making a determination on this?
- Similar issues with physical access and "immediate"- are we free to challenge FERC's order if we can justify rationale. DHS controls don't require immediate revocation.
- Timeframes should be consistent with the level of risk. Removing access? Do you need 6 months to do that?
- Keep in mind FERC directives are focused on the Version 1 standards. Directed to revise standards. Timeframes should be commensurate with risk through H/M/L. If speak to "immediate" we probably mean high.
- 6 months seems excessive.

Remote Access

- Controls apply across the board (215.24) pp 5.
- Pp 12- Passwords discussion- Frank's proposal- look at NIST material for password complexity and develop targets for h/m/l.

SDT Comments

- In Florida- interpretation of that requirement is that hardware enforces the password level.
- This is not in standards. Every requirement comes down to policy. NERC will need to address in the regions.
- Ask for unique (user name) identification and authentication? Remote access for high systems- low was just authentication.
- Use table- require a certain level of entropy etc.

- Caution the SDT in general against proposing a technology solution for high impact. Consider procedural mechanisms that may be stronger.
- New requirements pp 14- have no CIP corresponding requirement, e.g. authenticating management in DHS; mobile devices; wireless access in DHS; and time stamps for each group.

Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Dave Revill, Phil Huff (Lead) *Observer Participants: John Fridye*

Phil Huff reported on the Sub-Team's work reviewing the Change Management requirements worksheet. He noted that the Sub-team's work focused on the language itself, not on applicability. They still have to go through FERC order review. The have modified table/worksheet to track open issues/complications. They now have drafted most of the objectives and changes to CIP language.

Baseline Configuration
- Baseline of how configured for change control, for incidents and unauthorized

Configuration control
- Includes CIP 003 and testing

Access restrictions for configuration changes.
- Beyond access control. From DHS.
- Access control sub team may be sufficient.

Configuration assets-
- Configuration management plan- into policies and procedures.

SDT Comments
- Looked at the NISTER document? Yes, looked at NRC documents as well.

Information Protection
- CIP 003- section causing problems. Don't apply full protection program. Small subset of security controls applied to information. Chose to go that way again.
- Don't have confidentiality. Controls within requirements they are developing. Just protect your information. A bit vague, but lived with it so far and FERC hasn't commented.

Protection Program.
- Handling a new DHS procedures.

- Confidentiality agreements among entities.
- Assessment of program.

SDT Comments

- Confidential agreement protections- probably can't require. FERC doesn't have jurisdiction to require.
- Requirement can obligate the registered entity to put in place. Can't hold other side for compliance. That would be a contract relationship with a 3rd party.
- Good e.g. in other controls relating to Federal model. E.g. Inter-connected security agreement. Caution to the SDT not to bring in additional requirements grounded in federal model. Need to be sensitive to this and keep it "nice and Cippy."

Maintenance

- Periodic system maintenance- will combine with configuration management controls.
- Maintenance tools- prevent malware- detox without applying CIP controls to it.
- Maintenance personnel- authorized to perform maintenance on the cyber system (not cleaning crew).
- Remote maintenance- security controls above remote access- vendors or others performing some form of system maintenance.

SDT Comments

- Controls for when vendors log in for maintenance? Logging into sub system from main office is "remotely"
- Clarify with Sub-team on access control related to system maintenance? These are on top of control access requirements? Point of coordination.
- Remote maintenance- focus on who has access. Should be in the operations security group.

Media protection CIP 7 R7-

- Could have removable media (e.g. USB thumb drive to configure control systems). Make sure physically stored and transported securely. Disposal and secure for reuse.
- Define "media"? Field personnel to maintain accountability in terms of transportation of piece of equipment to a secure location and be wiped? Difficult to talk about security of data.
- Order 706- ability to erase media- this in direct odds with NIST- look at that.
- Make sure what is in equipment is no longer available when disposing equipment.
- E.g. Send Switzer back as it was in the failed state. Can't trouble shoot without being the same. They then send back a new one.
- Introduction of stuff into system. When take out, must do various things depending on the state laws. Stay away from info itself. Focus on info pertinent to our security. Don't worry about all information.
- Disposal- sending back to mfg.- data we want to remove vs. all other settings.
- Editorial- don't introduce programmatic requirement on entities as they apply to BES cyber system.

Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell

Jay Cribb reported on this group's effort including new BES cyber system component definition.

SDT Comment

- Discount unmanaged switches devices. Yes if a switch vs. a hub.

Boundary Protection/ESP

- New concept- problem with ESP- no such thing exists. Perimeter and access points.
- Only real things are the access point.
- Call "controlled boundary access points."
- ESP goes away.
- 1st Requirement
- Define boundary access points.

SDT Comments

- Boundaries between all BES cyber systems"? "Between each cyber systems and other systems"
- "Shared with other systems"? e.g. virtualized server environment.
- Around network switches- BES cyber system can't be existing in the same boundary as another cyber system. Substation e.g. Clarify this. Between BES cyber systems and non BES cyber systems.
- Trying to deal with this issue. ESP had bad traits for operations people. Flexible enough to be able to describe things as an entire system and looking at the boundaries between this. Addresses 706 order- more than perimeter- they talked about defense in depth. Boundaries not just a perimeter.
- Nice requirement. Simplified too much?
- First Requirements duplicates what is below. After shall: then all sub bullets and 2nd Requirement on boundaries.
- In/out is problematic word, however the intent is good.
- System definition will include the concept of a boundary. Don't want to have industry create boundaries don't exist.
- Applies to physical? Came from CIP 005- electronic boundaries.
- What does this mean in the physical sense?
- Clarify difference between ESP and boundary. Something to describe difference especially for industry that has spent resources identifying ESP.
- Need more "guidance" on what we mean by boundary.
- Will entity be free to describe how big or small that will be?
- "Boundary" may be viewed as a generic use of the term.

- Challenge trying to define a boundary (logically or physically). DHS says define the "external boundaries"- maybe that is enough.
- Cause confusion unless it clearly defines these terms. E.g. "shared component". Is boundary a filtering device?
- Clarify physical vs. electronic.
- Sub-Team tried to cover things at both the micro and macro levels.
- Change or rename the definition? Make sure boundary doesn't become a synonym for perimeter. "Access control points" is the focus.

Electronic Access Monitoring.
SDT Comment
- Manual process that logs and alerts unauthorized process? Consider taking out manual

Communications Integrity
- New under DHS catalogue and problematic.
- Clarify the objective
- Working connectivity into requirement.

SDT Comment
- CIP 004 Remote Access and CIP 007Account Management
- Some overlap regarding methods of authentification- Need to coordinate with Access Control group.
- Operation Security talks about where you need authentification. Access Control and Auditing sub-team will address how you do it?
- Mainly concerned with integrity of communication.
- Types of communication covered? "Wireless" good but some clarification of types.

Remote and Accessible Services (Port and Services)
- Objective
- R1
- R2 it is what it says today.

SDT Comment
- Strike technical since there might contractual.
- Document and implement compensating measures
- Issue of pre approval of compensating measures (TFE).

Flaw Remediation (i.e. DHS for Patch Management)
R1. Its what is there today with the terms re-named.
Malicious Software Prevention.
This requirements is a what. The "hows" are up to the entity. Will address in a guidance document.
Security Status Monitoring
R1- monitoring
R2- alerting (need applicability matrix here).
R3: Logging
R4 security event response

SDT Comments

- All events? All events related to cyber security.
- May not know until after.
- "Forensic"- may have legal implications. Maybe "post event analysis"
- Overlap with last one. Incident response team?

Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton

Jon Stanford reported on the Sub-Team's work reviewing the Requirements Worksheet. He noted that the right hand side includes the current CIP. He reviewed the opening checklist:

- Requirements are written at a high level. In general, seek to draft "what" and NOT "how", "specific" and NOT "prescriptive"
- Requirements have been developed using CIP-003-3 through CIP-009-3 as a starting point
- Applicable controls from the DHS Catalogue have been incorporated
- Changes from CIP-003-3 through CIP-009-3 have been documented
- Applicable directives from FERC Order 706 have been addressed

Security Policy and Procedures

- Overarching requirements- formal security policy(ies). Plural- One or more policies.
- a-d
- Capture DSH Management procedures and policies.
- XXX- subject area policies. Can place any policy language here.

Control System Security Plan

- One 1R with 3 subs: (a-c). Say what it is here. Go to security operations to get the details.
- 2R annually review each bes cyber system
- 3R- revise plan.

Security Plan Update

- Captured above

Control System Connections

- 1R: two parts.
- All connections authorized and documented.

Vulnerability Assessment and Awareness.

- 2 part Requirement.

SDT Comments on Governance

- Discreet requirements? Goal is a single policy. Is this a single requirement for a policy with bullets under requirements. Attachment providing elements?
- Each topical area could be listed by name or topic.
- Important thing: get senior management official managing the implementation requirements.
- Don't require only one policy and allow for internal program structure where it make sense.
- Eliminate overlap and duplication.
- No less than annually review your security plan for each cyber system? Didn't put update in.
- Security plan? Physical and electronic? No plan is for the BES cyber system.
- Look at your requirements- assume there are policies that say that will be done.
- Don't recreate policy statement.

IV. NEXT STEPS

The SDT reviewed the plans for the May 2010 Technical Workshop including Gerry Adamski's email. Gerry Adamski has offered to be the "general facilitator" for the workshop.

- How long? 1½ days. Move on location nailed and announcement to industry at large.
- Use the workshop- to have each sub-team- panel discussion 30-minute presentation. 30-45 minutes feed back.
- 12 hours of workshop time.
- Anticipate 500-1000 showing up to participate in the workshop.
- SDT team members show up. Planning day.
- Workshop objective is to get the SDT additional informal industry comment.

The Chair and Vice Chair noted that the Team had made a lot of progress over the course of the meeting. They reviewed the short term schedule for the Sub-teams. They will be meeting weekly as will the Sub-Team Leads to help coordinate the development of the drafts.
There is a lot of work to complete. Sub-teams may be scheduling additional working sessions and coordinating with Joe Bucierro. The SDT needs to enter its April meeting with a good draft
Sub-team should use Howard Gugel early and often.

The SDT requested that Friday sessions should clearly note if noon is the adjournment time so that members can make travel arrangements accordingly.

The Chair and Vice Chair and the SDT thanked Bill Winters for his excellent hosting and great facilities. Bill offered to host later in the year and will follow up with Joe Bucciero.

The meeting adjourned at 12:15 p.m.

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 20th Meeting Agenda
March 9, 2010, Tuesday- 1 PM to 5:30 PM MST
March 10, 2010 Wednesday- 8 AM to 5 PM MST
March 11, 2010 Thursday- 8 AM to 5 PM MST
March 12, 2010 Friday- 8 AM to 12 PM MST
Arizona Public Service CHQ
400 N. 5th St.
Phoenix, AZ 85004

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 revised CSO 706 SDT 2010 Work plan and Convergence Schedule Proposal
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and May 2010 Technical Workshop
- Review, discuss industry comments and identify issues raised to be addressed in revised CIP-002-4
- Review, refine and test consensus on a revised draft CIP 002-4 and Industry Response Document
- Receive progress reports for Security Controls Requirements Sub-Teams
- Develop and Test Sub-Team Security Controls Requirements
- Agree on next steps and assignments

Draft Agenda

Tuesday	**March 9, 2009**
1:00 p.m.	Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of February 16-19, 2010 Austin SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review and Discussion of CSO 706 SDT Workplan and Convergence Schedule - March-December, 2010- *Stu Langton*
1:45	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:55	Update on CIP Communication Plan and May 2010 Technical Workshop - *Carl Dombek*
2:15	Review of Revised CIP-002-4 Draft based on Industry and SDT Response to Industry Comments- *Draft CIP-002 Drafting Team, John Lim et al.*

3:00	*Break*
3:15	Continue review and discussion of revised draft CIP 002-4
5:25	Review of Proposal for Wednesday Agenda
5:30	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*
- *If needed, CIP-002 Drafting Team to meet to finalize draft and present for adoption Wednesday morning.*

Wednesday **March 10, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Review and Consideration of draft CIP-002-4 as revised and the Industry Comments Response Document
9:00	Sub-team Progress Reports and SDT Discussion of Key and Any Overlapping Issues

- Security Governance
- Personnel and Physical Security
- Operations Security
- Recovery and Response
- Access Control and Auditing
- Change Management, System Lifecycle and Information Management

10:30	Break
11:00	Review of Guidance and Overall Format for Security Controls Requirements Sub-teams
10:45	Sub-team Progress Reports and SDT Discussion of Key Issues- *Continued*
11:45	Security Controls Sub-Teams
12:00	*Working Lunch*
1:00	Security Controls Sub-Teams
4:55	Review Assignments and Thursday Agenda
5:00	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*

Thursday **March 11, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Security Controls Sub-Teams
10:00	Break
10:15	Security Controls Sub-Teams
12:00	*Working Lunch*
1:00	Sub-Team Reports and Full Team Consensus Testing on Refinements
3:00	Break
3:15	Sub-Team Reports and Full Team Consensus Testing on Refinements-*Continued*
4:45	Review Any Drafting Assignments and Friday Agenda
5:00	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*

Friday	**March 12, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Sub-Team Reports and Full Team Consensus Testing on Refinements-*Continued*
10:15	*Break*
10:30	Sub-Teams Reconvene to Review Refinements, Schedule and Assignments
11:00	Next Steps CIP 002 Drafting Group
11:15	Review of May 2010 Technical Workshop Planning and Preparation
11:45	Review and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

Appendix # 2 Attendees List
March 9-12, 2010, Phoenix, Arizona

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (Thurs)
2. Jay S. Cribb	Information Security Analyst, Southern Company Services
3. Jackie Collett	Manitoba Hydro (Wed/Thurs)
4. Sharon Edwards	Duke Energy
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation *(March 10-12)*
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Frank Kim	Hydro One Networks Inc.
10. Rich Kinas	Orlando Utilities Commission
11. Patricio Leon	Southern California Edison
12. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY
13. David Norton	Entergy *(March 9)*
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy
16. Kevin Sherlin	Sacramento Municipal Utility District
17. Jonathan Stanford	Bonneville Power Administration
18.Keith Stouffer	National Institute of Standards & Technology
19. William Winters	Arizona Public Service, Inc.
Roger Lampilla	NERC
Scott Mix	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

21. Jim Brenton	ERCOT
22. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Members Not Participating

Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co

Others Attending in Person

John Van Boxtel	WECC
Brian Newell	AEP
Clyde Poole	TDITX
Sam Merrell	CERT

Others Attending via WebEx and Phone

Andres	Lopez	andres.lopez@usace.army.com
Rod	Hardiman	rchardim@southernco.com
John	Fridye	jfridye@rrienergy.com
Keith	Walters	step@eei.org
James	Bassett	james.bassett@invensys.com
Steve	Newman	srnewman@midamerican.com
John	Van Boxtel	jvanboxtel@wecc.biz
Maggy	Powell	margaret.powell@constellation.com
Bill	Keagle	william.a.keagle.jr@constellation.com
Steve	Newman	srnewman@midamerican.com
Bryn	Wilson	wilsonwb@oge.com
Ray	Andrews	randrews@involta.com
Sam	Merrell	smerrell@cert.org
andres	lopez	andres.lopez@usace.army.mil
William	Keagle	william.a.keagle.jr@constellation.com
Bill	Glynn	bill.glynn@westarenergy.com
John	Allen	john.allen@cityutilities.net
Annette	Johnston	ajjohnston@midamerican.com

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 Subroups) 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 Subroups) 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 Subroup, as well as within the scope of the published agenda for the meeting.

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

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

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.

- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

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

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
JANUARY –DECEMBER 2010

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting-Atlanta, (4/13-16)	4/12/2010	**Present Controls draft for full team review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
	4/19/2010	**NERC Prepares Full Package for Industry Comment**
	4/26/2010	**SDT Reviews and Approved Full Package for 30-day Industry Comment Period**
5/3/2010	5/3/2010	***Informal Comment Posting for full package starts Completes on 6/2/2010***
SDT Meeting-Dallas, (5/11-14)	5/10/2010	**Prepare for Industry Workshop**
5/19 & 5/20/2010	5/17/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
	5/24/2010	**SDT Considers Comments from Workshop**
6/4/2010	*5/31/2010*	***2nd Informal comment period ends***
6/2/2010		***Comment Period Ends***
6/3-6/4/2010		***SDT Summarizes Comments Received***
SDT Meeting, Sacramento (6/8-11)	6/7/2010	**SDT Meeting: Comment review, response process, re-drafting, as needed**
	6/14/2010	Sub team meetings
	6/21/2010	Sub team meetings
6/29/2010	6/28/2010	Sub team meetings. SDT interim online meeting.
	7/5/2010	Subteams Package modifications into Standard documents
SDT Meeting, Pittsburgh, (7/13-16)	7/12/2010	**Finalize & Approve Documents for posting for 45 day formal comment period**

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
	7/19/2010	***NERC Prepares Materials/SDT Approves Revisions/NERC Seeks SC Approval for Ballot***
7/26/2010	7/26/2010	***45 Day formal comment period starts (completes 9/8/10) /Ballot Pool formation (completes 8/25/10)***
	8/2/2010	**Industry Comments on Standards**
SDT Meeting, TBD, (8/10-13)	8/9/2010	**SDT Meeting: Prepare for Industry Webinar**
8/18/10	*8/16/2010*	***Hold Industry Webinar***
8/25/2010	8/23/2010	***30 Ballot Preview/Initial Comment Preview ends/Ballot Pool formed***
8/30/2010	*8/30/2010*	***Initial Ballot Starts***
SDT Meeting Winnipeg, (9/7-10)	9/6/2010	**Respond to comments received. Drafting revisions. Review Ballot Results and Additional Comments**
	9/8/2010	**Initial Ballot Ends**
	9/13/2010	Sub team meetings
9/24/10	9/20/2010	Sub team meetings; Full SDT on-line meeting to adopt revised draft of documents
	9/27/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
10/4 to 10/13/10	10/4/2010	Re-Ballot Period Begins
SDT Meeting TBD, (10/12-15)	10/11/2010	**Prepare responses to 2nd ballot comments**
10/19/2010	*10/18/2010*	***Sub-teams meet to adjust requirements***
10/29/2010	10/25/2010	***Prepare & Finalize revisions to standards and responses to comments on standards***
	11/1/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
11/8 to 11/17/2010	11/8/2010	3rd Ballot Period Begins

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting TBD, (11/16-19)	11/15/2010	**Prepare responses to 3rd Ballot comments**
	11/22/2010	*NERC & SDT finalize responses to ballot package*
	11/29/2010	*Seek SC & BOT Approval for Filing*
	12/6/2010	*Seek SC & BOT Approval for Filing*
SDT Meeting TBD, (12/13-17)	12/13/2010	**SDT Meeting to review Filing and Celebrate Project Completion**
	12/24/2010	*Submit for Regulatory Approval*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #5

CSO 706 SDT DRAFTING SUB-TEAMS AND DRAFTING GUIDANCE

Sub-Team	NERC Standards and DHS Control Families	Team Members
Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton
CIP 002-4	Draft revisions to CIP-002-4, and Summary of Responses to Industry comments	John Lim, Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton *Rod Hardiman (Observer)*
Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell
Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*
Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Phil Huff (Lead) *Observer Participants: John Fridye*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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.