NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

January 19, 2010 | 1:00 p.m. to 5:00 p.m. EST
January 20, 2010 | 8:00 a.m. to 5:00 p.m. EST
January 21, 2010 | 8:00 a.m. to 5:00 p.m. EST
January 22, 2010 | 8:00 a.m. to 5:00 p.m. EST

Adopted Unanimously by the SDT February 18, 2010

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

Joe Bucciero, Bucciero Consulting, LLC

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary Contents

EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. On Thursday morning the SDT approved without objection the meeting summary for the December, 2009 meeting in Little Rock.

The Chair thanked members for their diligence, dedication and participation through the holidays to prepare the finalized draft of Version 3 of the CIP-002 to 009 Standards for balloting. Stuart Langton reviewed the SDT work plan, in particular the parallel effort of developing security controls while preparing Version 4 of the CIP-002 standard for posting for an informal comment period. The Chair noted this was her last meeting on the Team and that Jeff Hoffman from the Denver Office of the U.S. Bureau of Reclamation was being recommended to the NERC Standards Committee to serve as a member on the SDT. Joe Bucciero noted that Christopher Peters has submitted his resignation from the Team, and that Patrick Leon (Patricio Leon Alvarado) from Southern California Edison is also being recommended to serve as a member of the SDT. Mr. Bucciero noted there are two remaining open SDT member positions and invited members to talk with potential candidates and have them submit membership nomination forms.

Joe Bucciero provided an update on CIP 002 filing process and some reflections on lessons learned. He recounted that the NERC standards managers reviewed and discussed format and other changes to the standards following the SDT adoption of the CIP002-4 draft in Little Rock. Due to the press of the holidays and the FERC imposed deadline for posting, there was little time available to communicate with the SDT leadership and team members regarding the rationale for the NERC proposed changes. NERC agreed to withdraw many of the proposed text changes and submit them as comments during the informal comment period. Going forward, NERC has assigned Howard Gugel to the Team so he can improve coordination with NERC standards managers and provide direct format assistance in the Team's drafting process.

The Chair noted that yesterday Dave Norton circulated to the Team the release of a preliminary draft of the NIST Interagency Report (NISTIR) regarding the work of the Cyber Security Coordination Task Group (CSCTG) established to help define the cyber security requirements for the smart grid. The NISTIR document is planned to be finalized later this Spring. Keith Stouffer noted that there are over 300 people with seven working groups involved in the CSCTG. It will become a standing committee that is part of the Smart Grid Interoperability Panel (SGIP) that has been created by NIST as part of their work in response to EISA 2007. Keith also noted the draft NIST interoperability roadmap was recently released on January 19.

Gerry Adamski, director of NERC Standards noted he is working with the new NERC Communications Director, Carl Dombek and will share a draft plan with the Team later in the week. The Chair suggested that Carl Dombek be able to come to a future SDT meeting to brief the SDT and provide an update on the progress with implementing the communication plan. The Team agreed that the industry webinar addressing the draft CIP-002-4 standard should take place on February 3 from 1:00-3:00 p.m. EST to allow for industry feedback and questions on the new approach to this standard. SDT Vice-Chair, Phil Huff, agreed to serve as the contact for the Team's effort in developing the webinar materials, and Sharon Edwards and Jay Cribb will be the SDT presenters for the webinar.

On Tuesday morning, Scott Mix and Howard Gugel from NERC briefed the Team on the development of a security controls drafting template.

Phil Huff provided an overview of the SDT effort since Little Rock to develop a draft strawman including development of a security controls member survey created by the SDT leadership; a summary of the responses to the survey by 16 members compiled by the staff; a SDT conference call on January 6, 2010 to consider the member survey results and create and charge a drafting group; and two strawman drafting team meetings were assigned to develop a strawman document. The strawman document contained: Security Control Drafting Principles to provide guidance in drafting security controls and ensure more consistent outcomes among sub-teams; Security Control Groups having the relevant CIP 003-009 and NIST SP 800-53 families mapped including: Security Governance; Personnel and Training; Communication Protection; Physical Security; Systems Management; Incident Response; Recovery Plans; Access Control (Technical); Audit and Accountability; Configuration Management and System Lifecycle; Information Management; and Security Assessments.

Phil Huff noted that the first ten principles are drawn from NERC rules of procedure. The Team reviewed principles 11-15 and offered suggestions for refinements.

Phil Huff outlined the control group categories in the strawman draft. The Team reviewed the proposed six sub-teams in the strawman document including: Security Governance; Personnel and Physical Security; Operations Security; Recovery and Response; Access Control and Auditing; and Change Management, System Lifecycle and Information Management. On Tuesday morning sub-team preference forms were distributed to the members in the room and electronically to those participating via the Ready Talk conference facilities. Based on the preference form, the Sub-Teams were created.

Phil Huff reviewed the strawman guidance for the sub-groups. Following the initial Sub-Team reports on Wednesday, the Team discussed the implications for the ultimate standards/control format and for the further development of security controls in the context of CIP-002-4. On Thursday morning, the Team discussed whether the proposed "control group" format should be the organization for revising the current CIP 003-009 or just a starting point for the Team's work on security controls. The Team discussed the strengths and weaknesses of three choices going forward: using the current CIP Standards, the NIST SP 800-53 format, or the DHS security controls structure. Following the discussion, the Team considered and tested a fourth option of preparing the requirements first then determining the format going forward. Using the following 4-point acceptability scale, the Team decided to proceed first to create the requirements and controls and defer the format options review until having completed that task.

Prepare Requirements First, then Decide on Format

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	9	**6**	**0**	**1**	**3.3 of 4**

The Sub-Teams met on Wednesday morning and early afternoon and then reported their initial results on the review of selecting candidate controls from the DHS catalogue. The Sub-Teams met for a second time on Thursday morning and early afternoon to review security controls and begin exploring the drafting of requirements.

Prior to the second sub-team break-outs on Thursday morning, the Team agreed on a sub-team format for collecting information with the following columns:

1. SDT Team Name
2. Section #
3. Title
4. NERC Security Guidance
5. NERC CIP-2
6. NIST SP 800-53
7. CSO 706 SDT Applicable
8. SDT Comments
9. Validated 706 SDT Applicable (Yes/No)
10. Existing CIP Requirement Cross Reference
11. FERC Order 706 References (Paragraph #s)
12. Requirement Definition
13. Controls- High
14. Controls- Medium
15. Controls- Low
16. Applicability- Transmission
17. Applicability- Generation
18. Applicability- Control Centers

Over the three days the sub-teams met first to identify candidate DHS Security Controls and then to identify controls and draft requirements. The sub-teams and their members included:

1. Security Governance and Assessments *(Gerry Freese, Jon Stanford, Rich Kinas)*
2. Personnel and Physical Security. *(Doug Johnson, Rob Antonishen, Kevin Sherlin).*
3. Operations Security *(Jay Cribb, John Varnell, Jackie Collett & Jim Brenton)*
4. Recovery and Response *(Jeri Domingo Brewer, Jason Marshall, Joe Doetzl, Scott Rosenberger)*
5. Access Control and Auditing *(Sharon Edwards, Phil Huff and Jeff Hoffman)*
6. Change Management System Lifecycle and Information Management. *(Dave Revill, Keith Stouffer and Bill Winters)*

On Friday morning, following the sub-team reports, the Team offered reflections on the sub-team exercise. Following the sub-team reports, the facilitators presented and the Team reviewed and refined the next steps and assignments emerging from the meeting including steps for the Team as a whole, security control sub-team assignments, and steps in the CIP-002-4 review and refinement process.

Scott Mix presented a revised proposed schedule for CIP 002 and the security controls requirements *(See Appendix #5).* The Team liked the presentation in which the two efforts are put in parallel columns and shows the amount of work ahead.

Vice-Chair, Phil Huff reviewed some questions that the Team discussed for FERC/NERC meeting on January 28, 2010, including:

1) What expectations are there regarding coordination with the Smart Grid CSCTG (Cyber Security Coordination Task Group) product and how we use NIST SP 800-53/DHS Catalogue?
2) NIST SP 800-53 is an organizational risk management framework, which allows for tailoring and compensating controls. However, FERC Order 706 calls for extensive oversight for any exceptions. What are their thoughts on reconciling these seemingly conflicting objectives?
3) The process to make modifications to the Standards through a FERC Order is very resource intensive. Conversely, changes made prior to industry balloting are done with relative ease. Is it possible to have a process where the team can receive feedback from FERC prior to ballot?
4) To what degree can we remove or lessen prescriptive elements in the current CIP Standards where the risk reduction does not justify the consumption of industry resources?
5) Have we captured all of the directives from Order 706 in the filing made in December 2009?

He noted this was a working list which will be circulated for members to suggest additions in advance of the January 28 FERC/NERC meeting.

The facilitators noted that each sub-team should plan on meeting in the interim (between meetings) and on preparing and presenting at the February 2010 meeting in Austin a short progress report including key questions for presentation. The Austin meeting will primarily focus on refining CIP-002-4 in response to industry comments received from the informal comment period (ending February 12). NERC will try to have Maureen Long attend a portion of the Austin meeting (preferably on Thursday) to address the response and refinements of the CIP-002-4. The primary objective of the Austin Meeting is to have the Team reach agreement on CIP 002 as revised for posting for 45 day formal comment period.

On behalf of the SDT, Phil Huff thanked Jeri Domingo Brewer for her leadership over the past 16 months. Ms. Brewer acknowledged the opportunity to get to know the SDT members and noted the honor of having worked with them to produce excellent and timely outcomes. She urged the Team to continue to build on the foundation of trust and collegiality to complete the task assigned by December 2010.

Mr. Huff then thanked Dave Revill for hosting the meeting and providing excellent support for this critical meeting.

The SDT adjourned at 12:30 p.m. on January 22, 2010. Several sub-teams continued to meet following lunch on Friday afternoon.

MEETING SUMMARY

I. AGENDA REVIEW, WORKPLAN, UPDATES AND COMMUNICATION PLAN

A. Agenda Review

On Tuesday afternoon, the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the December, 2009 meeting in Little Rock.

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

The Chair thanked members for their diligence, dedication and participation through the holidays to get the draft finalized and ready for balloting. Stuart Langton reviewed the SDT work plan (*See Appendix # 5)* in particular the parallel effort of developing security controls while finalizing the CIP-002 draft for balloting.

The Chair noted this was her last meeting on the Team and that the Standards Committee was going to appoint Jeff Hoffman from the Denver Office of the U.S. Bureau of Reclamation to serve in her stead. Joe Bucciero noted that Christopher Peters had submitted his resignation from the Team. The Standards Committee has appointed Patrick Leon (Patricio Leon Alvarado) to the SDT from Southern California Edison, who has the lead for CIP NERC compliance in terms of their substations and also has considerable substation planning experience. He will join the Team at its Austin meeting. Mr. Bucciero noted there were two open spots and invited members to submit potential candidates.

B. Lessons Learned- CIP-002-4 Posting

Joe Bucciero provided an update on CIP 002 Filing process and some reflections on lessons learned. He noted that much has been learned since this Team was formed in the Fall of 2008. He recounted that the NERC standards managers following the SDT adoption of the CIP002-4 draft in Little Rock reviewed and discussed format and other changes to the standards but due to the press of the holidays and the deadline for posting did not adequately communicate to the SDT leadership and team members the rationale for proposed changes. NERC agreed to withdraw many of the proposed text changes and submit them as comments in the informal comment period.

Going forward, NERC has assigned Howard Gugel to the Team so he can improve coordination with NERC standards managers and provide direct format assistance in the Team's drafting process. Joe Bucciero agreed to circulate to the Team documents that lay out the new approach for standards drafting. Mr. Bucciero noted that NERC's leadership change with a new President stepping in was a factor.

Member Comments

- Going forward the Team will be struggling to get the documents to a point we can agree on them as a group – there may not be enough time for NERC staff review – may need to change the

process to allow for staff review and then committee review and agreement before it goes to ballot.
- We should not face this in the future since Howard will to help coordinate the issue to reduce the problem in the future

C. Cyber Security Initiatives Updates
The Chair noted that yesterday Dave Norton circulated to the Team the release of an intermediate draft smart grid work of the Cyber security coordination task group to be finalized later this Spring. Keith Stouffer noted that there are over 300 people with seven working groups. It specifies security standards at multiple points and is a list of requirements rather than baselines. Keith also noted the NIST roadmap for operability was also just released on January 19.

Member Comments
- Need to continue to coordinate between our group and theirs to be sure not developing incompatible requirements
- The Team may want to consider forming a task group looking specifically at the Smart Grid work to be sure our work is compatible and not at odds or creating issues.
- Add agenda item for Wed. or Thurs. for discussing how we can interact or interface with that group?
- Can we feed our work back to that task force as we move forward?
- Another item – critical cyber security identification guideline is now out for formal comment. This is a formal guideline development process, not a standards development process despite the similarities.
- U.S. nuclear plants – NERC needs to file version 2 implementation plan – how version 2 and 3 will be applied to nuclear plants – Commission says implement on same time line as version 1 – The order says future orders must include how nuclear plants are expected to apply

D. NERC Update on Implementing the CIP Communication Plan
Gerry Adamski, director of NERC Standards noted he is working with the new NERC Communications Director, Carl Dombek and will have a plan to share with the Team later in the week (*See Appendix #9)*. He noted the need to set a date for a CIP 002-4 webinar in early February. He noted that NERC is not expecting this Team can take the lead in developing and implementing a communications plan. The Chair suggested that Carl Dombek may be able to come to a future SDT meeting to brief and provide an update on progress with implementing the communication plan. The Team agreed the webinar should take place on February 3 from 1:00-3:00 p.m. EST to allow for industry questions. SDT Vice Chair, Phil Huff, agreed to serve as the contact for the Team's effort in developing the webinar materials. Sharon Edwards and Jay Cribb will be the SDT presenters.

E. Review of NERC's CIP Security Controls Drafting Template
On Tuesday morning, Scott Mix and Howard Gugel from NERC briefed the Team on the development of a security controls drafting template. Mr. Gugel noted that one key is for the Team to decide how much granularity they want to work with and suggested it will be easier to start with the broader high-medium-low categories. He also pointed to using a table format that would be referenced by each requirement. Other points made included:

- Requirement statements can be very short and simple: e.g. you shall implement passwords subject to attachment # 1. The entity looks in the attachment to determine if you are high, medium or low, then look at details for compliance. There remains a question as to whether compliance is assigned to a column or row versus to an individual cell in the table.
- Requirement could speak to applicability and the attachment would catalogue the controls.
- The example is divided just to indicate whether or not you need different types of controls for transmission, control centers, generation, etc. It also breaks it down to look at whether it is manned or not which may affect the mapping of controls needed.
- Third example is just "high BES impact" with granular of physical access, monitor physical access or logging physical access
- Control centers have a lot more for virus protection than a remote center – then break it down into transmission, production or control – don't need virus protection of a relay (though those with windows platform may need some)
- The Team should consider the VSLs as you are writing requirements – if not, there is a disconnect and you may find you did not write the requirements as clearly as you should have
- The proposed concept will work best for this Team and this is the direction overall NERC and the industry needs to be headed in. In addition it is easier to follow.

Member Comments

- Suggesting just one VSL level for each of the h-m-l categories? No – associated with each requirement is a set of VSLs
- Each violation has a risk factor – but this is not a one-to-one relationship.
- Do you have a prototype we can look at? Not yet.
- We need to look at the violation severity and have clear cut controls. 90% of the effort should then be aimed at highest level impact.
- If it is a high impact it needs to be protected. It should not be important to determine whether it is transmission or control center or other. It is the impact on the BES that is important.
- I like idea of doing the VSLs at the same time to allow us to fine tune the requirements and be sure they are auditable.
- This just shows how to map each requirement – may not have a direct tie to a VSL
- Are these several different models to use together or are we choosing one over the other?
- The concept is good – this might be useful once we decide which controls are in the buckets of h-m-l. Your suggestion makes implementation simpler.
- If you have a table do you still have just one requirement or does the table represent Sub-Requirements? This is an open question at this point
- Is there a NERC style guide for VSLs we should reference? There is but it does not assume the complexities of what we are looking at here.
- I think the VSLs need to be more granular than the requirements. VRFs should be easier to assign to impact levels than VSLs.

- We should consider creating a litmus test to use as we move forward.
- Should we count one miss the same as multiple misses of the requirement?

II. SECURITY CONTROLS AND THE STRAWMAN DOCUMENTS

A. Overview of Security Controls Strawman Document and Drafting Group Process

Phil Huff provided overview of the SDT effort since Little Rock to develop a draft strawman. This included a:

- Security controls member survey developed by the leadership in December, 2009;
- Summary of the responses by 16 SDT members compiled by staff, *(See Appendix # 6),*
- Full Team conference call on January 6, 2010 to consider the member survey results and create and charge a drafting group, and
- Strawman drafting team which met twice on January 11 and 14, 2010 to develop and bring a strawman document to this meeting for the Team's consideration.

He thanked the Team and the drafting team members for their responsiveness in completing the survey and developing a strawman document (*See Appendix #8).* The strawman document contains:

1. Security Control Drafting Principles to provide guidance in drafting security controls and ensure more consistent outcomes among sub-teams;
2. Security Control Groups having the relevant CIP 003-009 and NIST SP 800-53 families mapped including: Security Governance; Personnel and Training; Communication Protection; Physical Security; Systems Management; Incident Response; Recovery Plans; Access Control (Technical); Audit and Accountability; Configuration Management and System Lifecycle; Information Management; and Security Assessments
3. Drafting Sub-Teams based on the control families:

Team	Control Families
Security Governance	(1) Security Governance
Personnel and Physical Security Operations Security	(2) Personnel and Training, (4) Physical Security (3) Communication Protection, (5) Systems Management
Recovery and Response Access Control and Auditing	(6) Incident Response, (7) Recovery Plans , (12) Security Assessments (8) Access Control, (9) Audit and Accountability
Change Management, System Lifecycle and Information Management	(10) Configuration Management and System Lifecycle, (11) Information Management

4. Team assignments to determine the security controls within their assigned control families necessary to mitigate risk to the BES. Begin by taking the set of applicable Requirements from version 3 CIP Cyber Security Standards and reconcile with applicable NIST SP 800-53 security controls. Then incorporate additional sources where applicable to mitigate unacceptable risk to the BES functions. The initial work product should be a set of security controls with applicability to high, medium and low impact Cyber Systems and how specific FERC directives have been

addressed *(as indicated in Appendix A: FERC Directives from Order 706).* Additionally, for each security control:

- State how the security control reduces risk appropriate to the impact categorization *[Drafting principle 11]*
- State how an objective third party with knowledge or expertise in security can measure the control *[Drafting principle 4]*
- State the rationale for making changes from previous versions [*Drafting principle 12]*
- Denote the applicability to (1) Generation Subsystems, (2) Transmission Subsystems, and (3) Control Centers. Provide clarifications or enhancements where necessary to meet the security control objective in that environment *[3.2 acceptability among survey respondents]*.
- Denote the priority for the security control relative to the risk it mitigates (i.e. P1, P2, P3, None). *[SP800-53 introduced this in version 3, and it could help in developing VRFs and implementation plans]*
- Denote applicability for differing vulnerability and threat profiles.
- Write controls based on risk profile (as well as impact categorization)
- Denote applicability for general purpose vs. proprietary operating systems.

5. Security Controls for Impact Categories with basic premise that the cost to implement security controls should reflect the reduction of risk to the BES commensurate with the impact category. The industry as a whole should first focus on mitigating the greatest amount of risk.
6. NERC CIP/NIST SP 800-53 will serve as the baseline and SANS, ISO, DHS, and ISA-99 provide supplemental or amplifying guidance.

B. Drafting Principles

Phil Huff noted that the first ten principles are drawn from NERC rules of procedure. The Team reviewed 11-5 and offered the following suggestions.

11. Reduce Risk [**3.5 acceptability among survey respondents**] **–** Security controls reduce risk appropriately for applicable BES impact categories.

Member Comments and Suggestions

- Depend on an entities implementation? Yes, but assume that we will be making risk decision of what is minimum acceptable for reducing risk as we develop the standards.
- This one deals again with what is high, medium and low.
- Throwing around "risk" a lot – There is a complaint that we use "risk" but cannot qualify it, nothing to document what we are doing reduces "risk" – show me how it is a "risk"? How do we justify using the word if we cannot quantify it
- Same problem with #11 – current standards assume a positive benefit from any effort to reduce risk – in federal model you perform risk assessment and decide whether what you are doing is acceptable.
- Need to clarify the level of organizational risk that applies – but have to have an industry baseline and justification that this is appropriate and reduces risk as we understand it in the industry.
- What are the threats we trying to counter so we know what to put into place to address it
- As we identify a control, we must assume controls reduce risks?

- We cannot do a risk assessment for the whole industry.
- Discussing the outcomes of having controls – this may be the overarching goal, rather than a principle.
- May need to define "reduce risk" – what is the intent of the controls? Reducing risk may be an outcome
- The list is intended as measure of review of the draft products of each group.
- Under the survey the question asked if it would be appropriate to document how the controls reduces risk. That is covered in the next section
- Cannot prescribe controls and quantify specific results – it is the controls as a whole?
- My concern is with the word "reduce." Reducing from what? Have to have a starting point.
- Talking about overarching principles which is fine but on page 4 asking each group to begin with a statement of the risk and we may get back into the circular argument – need to establish and clarify why we are offering a control. We will need to have some reason why requiring the industry to do this.
- If we do this for every control, we may get bogged down given the 200+ items listed – may simply need the justification for a category of controls rather for than each individual control.
- We need sound reasoning for why we are or not including a security control.
- We need to be sure we are not expecting a control to reduce a high risk impact is also applicable to a low impact item too.
- Need a principle that we need appropriate controls that are applicable to a category – controls that are appropriate and applicable – rephrase the principle so as not to lose that thought?
- Is #11 the same as #14? Not the same, as #14 is intended to avoid all of the compliance effort being aimed at low levels.
- "Security controls shall be appropriate for applicable BES impact categories."
- "Security controls shall be commensurate with identified level of BES impact categories."
- As a guiding principle this is fine – the Team understands the intent of this principle.

12. **Change Documentation** [**3.3 acceptability among survey respondents**] – 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
    c. Major formatting changes.

Member Comments

- We cannot pass anything that doesn't give a roadmap from how to get from version 2 to 3 to 4 – if we drop something along the way we need to justify it.
- May want to test and get validation from NERC staff before finalizing – make this part of the communication plan? Note that staff cannot speak for the commission
- Industry will want to know why it appears we have gone from asking them to do 40+ things to 200+ things – may be the same or less total work even if more items.

13. **Reduce Administrative Overhead** [**Suggested principle**] **–** Administrative documentation kept to the minimum that is necessary to verify acceptable risk.

Member Comments

- How do you measure compliance? If you reduce documentation? NERC and regions may make up what you need. We should be all for reducing documentation, but we have to show compliance.
- Currently, you are out of compliance unless through documentation you can prove you are in compliance.
- Documentation needs to be rational but we probably cannot completely eliminate documentation.
- No matter how much documentation we have, it seems it is never enough to completely prove compliance – documentation is always subject to interpretation. We must make this more precise
- As worded the principle is what you want – have to have adequate documentation but not more than needed.
- Cut off the principle after "necessary"?
- Also federal performance audits actually improve security.

14. **Priority [Suggested Principle] –** Implementation and compliance with the Standards are prioritized according to BES risk. The industry should focus on mitigating the greatest risk (i.e. not spend the majority of our resources on the low-impact Cyber Systems).

Member Comments

- We can't just bite off little parts – adding priorities may be done differently depending on your processes.
- Priority built in already – is this going after impact levels rather than risk? Prioritize based on BES impact. Prioritizing could be handled through the implementation plan followed by a compliance plan.
- Need to just remove – already categorizing into high, medium, low – that set priorities, still have to get to the low too.
- Replace "risk" with "impact" – how do we focus on "high impact" to get most bang for the buck. It may important enough to do, but perhaps not important enough to test? Simply remove "and compliance" from the sentence?
- *(*Parking Lot item)* Can small entities leverage the work of others? Should we allow them to? Ballot body may be more amenable if we do this.
- What is the mechanism that allows them to do that since audits cannot be shared?
- These are principles for the Team to use moving forward, and are not for the industry: strike the second sentence?

15. **Minimize TFEs** [**Suggested principle**] **–** Security controls should minimize the need for TFEs

Member Comments

- What is the principle or goal? To eliminate TFEs? It is clear that the TFE process is broken – should be striving to eliminate the need for TFEs.
- TFEs were an end run on the requirements – reword standards to eliminate the need for an "end run."
- Allow for controls to mitigate and document for older equipment that cannot meet all the requirements – call it whatever you want.
- TFE is an existing term and process – eliminate the need for TFEs – replace with an effective exception process. We will still have a need for exceptions. Add compensating controls?
- TFE grants safe harbor from retroactive sanctions – can we write any exception without such retroactive protection? Are we constrained by the current process? This is a question for NERC.
- "Mitigating controls" vs. "Compensating controls" are very different terms.
- There may be a place for exceptions, but not the current TFE system that has been misused.
- Reasonable to expect there will need to be some exceptions – we cannot write a standard that will cover all possibilities.
- Issue is over the word "exception" rather than the concept or need for them. We know there will be instances where an entity cannot meet the letter of the standard – remember these standards are mandatory.

C. Control Group Categories

Phil Huff outlined the control group categories that the strawman draft proposed depicted below:

ID	Control Group	NERC Standard	NIST SP 800-53 Family
1	Security Governance	CIP-003 – R1, R2, R3;	Planning, Risk Assessment, Program Management
2	Personnel and Training	CIP-004 – R1, R2, R3	Awareness and Training, Personnel Security
3	Communication Protection	CIP-005 R1, R3	System and Communication Protection
4	Physical Security	CIP-006 R1 through R6	Physical and Environmental Protection
5	Systems Management	CIP-007 R2, R3, R4, R6	System and Information Integrity
6	Incident Response	CIP-008 R1 & R2	Incident Response
7	Recovery Plans	CIP-009 R1 through R5	Contingency Planning
8	Access Control (Technical)	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4	Access Control, Identification and Authentication
9	Audit and Accountability	CIP-005 R5, CIP-007 R9	Audit and Accountability
10	Configuration Management and System Lifecycle	CIP-003 R6; CIP-007 R1, R7	Configuration Management, Maintenance, Media Protection, System and Services Acquisition
11	Information Management	CIP-003 R4	Access Control, Media Protection
12	Security Assessments	CIP-005 R4, CIP-007 R8	Security Assessment and Authorization

Member Comments

- Number 12, Security Assessment should be moved up as part of Security Governance (#1)? Yes.
- Access control in #11 different from that in #8? Access to information versus access to systems. Remove access control from #11 as both uses of term covered under CIP 003 R5 in #8.

D. Proposed Sub-Teams

The Team reviewed the proposed six sub-teams in the strawman document including: Security Governance; Personnel and Physical Security; Operations Security; Recovery and Response; Access Control and Auditing; and Change Management, System Lifecycle and Information Management. On Tuesday morning sub-team preference forms were distributed to the members in the room and electronically to those participating on ready-talk. *(See Appendix # 7 Preference Form results).*

Member Comments

- Recognize that the six categories may leave only a couple members per team among members physically present
- Consider combining access controls and operations security?
- Consider having members serve on more than one group? Especially any categories that may need coordination?
- How can we account for those with time available for the group and those who don't? Careful we don't end up with a group of three but none have sufficient time to complete the task.
- Several mappings or cross walks exist already.
- May need to review mapping together as a team to start, then break off to deal with sub-questions
- Would it be beneficial to go through DHS(?) catalogue rather than NIST SP 800-53?
- Mapping exercise? Pull up a control and ask if it is applicable?
- Should we be working toward identifying the plan or approach first?
- Would discussion of High/Medium/Low happen with the mapping discussion?
- What is in the CIP now generally is the high – pare down from there to identify medium – then low.
- We need to draw on varied experiences in the Team to draw conclusions and map the controls. We also need to develop a common understanding by drawing on the groups experience
- Why are we defending against any standard? We were asked to consider NIST, not defend from it?
- Trying to identify gaps and explain why we did not include a particular control or standard
- Simply need to explain why we did not include a type or group of controls
- NIST is a different way of doing things, not directly comparable with existing CIP standards.
- I agree they are different – but looking at different references for ideas that may improve coverage. We should not be looking to make wholesale changes if we don't have to.

E. Review of Required Elements for Each Security Control
Phil Huff reviewed with the Team the strawman guidance for the sub-groups.

Member Comments

- The strawman guidance on high/medium/low was intended to simply offer an example, and is not trying to write the control
- Use high category and pare down from there?
- High/Medium/Low may mean different things when looking at control center versus a transmission subsystem.
- Medium will be a tough category to define.

- E.g. Passwords. May want shorter passwords changed less often for low than for high. The requirement is to use passwords for authentication – do you define the complexity for the level of impact?
- Consider establishing a short succinct requirement and then look to the column and row in the attachment tied to the level of impact.

III. SECURITY CONTROLS FORMAT AND SUB-GROUPS

Following a mid-morning break on Wednesday, the Team reviewed sub-team assignments and then broke out into sub-teams to initially review the DHS catalogue of controls to determine the applicability of these controls to their sub-group categories. On Wednesday afternoon the sub-groups provided initial reports.

A. Initial Format Discussion

Following the reports the Team discussed the implications for the ultimate standards/control format and for the further development of security controls in the context of CIP-002-4.

Overall Comments following Initial Sub-Group Reports on Wednesday

- No equivalency requirements in this one. Looked at requirement and supplemental guidance.
- With a CIP requirement- take side by side. Look for what is different
- JS: FAQ- "access point" defines ESP. Providing traffic control in/out of ESP. Have to have fire wall. Access control-
- Access control and monitoring- on DHS- access control pp 93. Identification authentification of a use etc. for granting access to user. Combine and you have access, authorized access. 3 stages of the process.
- How IT/cyber security- access control. Without a NERC definition of "access control"
- "Network perimeter protection"- visuals upper management. "Guards, gates and guns"- physical and virtual perimeters to explain without jargon.
- Identification and authentification- problematic do not exist in any legacy or modern in any SCADA, ill defined. There will be lots of discussion around this issue. It is possible to authenticate and identify?
- Why no "access control" definition? Disappointed with small number of defined terms.
- Parking Lot issue: Access control.
- Remote access through an ESP. After spot audit. This is an important issue. We need to deal with universally understood concepts, understood the same way. Get away from concepts understood only by a drafting team.
- The problem may be who accepted it?
- NERC defined terms- if we put them in a reference document, they will not be part of the standard.
- Different approach – said yes to good ideas but recognize may be difficult to write a requirement – we did not look to see if already in the CIP, just whether it should be considered "high."

- Go back and agree on the criteria for high, medium, low and then repeat the review to categorize the ones identified by the sub teams.
- Should we have a first draft of the total bucket and then refine the issues? We can then use a standard template to redact high, medium, low.
- Take work done today through a next step to look at words surrounding the possible requirement
- Need to talk about format – how are we going to structure the requirements moving forward?
- Make a change to one standard it ripples through the others – can we make these stand alone? I need more information on how we are going to structure the standard to avoid tripping over each other in sub teams.
- Take one family – a smaller one – and develop a "proof of concept" for putting into a table to establish a template for the other larger families
- Collapsing to smaller number of requirements? Caution, the smaller the number of standards, the more likely we will be out of compliance with a standard.
- Out of compliance with a requirement, not just a standard?
- Agree we should work on one to establish the standard.
- Which one should we utilize?
- The Team should take the .1 in each DHS family as policy to be addressed in the Governance
- We will need to address when a control family crosses over multiple areas
- Need to work on getting requirements into a new format or framework – but collectively need to discuss how to construct the bucket. I.e. what is the control framework? What is preference and what builds clarity and understanding?
- If keeping CIP 003-009, do we keep the policies spread through each or pulled out into a separate stand alone
- May depend on who the target user of the document is – target to field, management, others?
- How do we address generation, transmission or control centers? One size does not fit all – they each have unique requirements – need to make it easy to look up transmission requirements for example.
- Think about the NERC development process and that you need to sell this to through the ballot process to the industry – start with existing and refine and modify from there – otherwise much more difficult to sell to industry
- Our drafting principles call for keeping it close to current structure.
- Page 3 of strawman has a suggested structure in the chart – current CIP003-009 into control groups.
- Small group meet after we adjourn to discuss and develop a starting point for tomorrow's discussion
- Also need to compile the "yes" and "maybe" from the sub teams
- Not suggesting throw the whole structure out but collect common policies together first – shouldn't worry about whether they map one-to-one with current structure – putting policies

together will help us sell to industry the changes – elevate policy and bucket the rest of the controls into appropriate sections

B. Consideration of Security Controls Format Options

On Thursday morning following the sub-groups' first round of meetings on Wednesday afternoon, the Team discussed whether the proposed "control group" format was being proposed as an organization for revising the current CIP 003-009 format or just a starting point for the Team's work. The Team discussed the choices going forward, initially identifying three: using the current CIP, the NIST SP 800-53 format or the DHS security controls structure.

Member comments

- Do we need to have some motion or vote to determine the form we are moving forward
- Need a good strong framework to build on – need to determine today what we will use as the structure – move the pieces around using the structure we have or create a new structure – we struggle with the existing structure – don't like the idea of just moving the deck chairs around – need to resolve and get it behind us
- Need to discuss strengths and weaknesses of each and may need to recognize that option that is not favored may still have an element we want to incorporate
- The Team was called together to fix problems identified by FERC. We need to fix those with the tools available including NIST – order did not call for a change in structure – people are familiar with it and likely to vote in favor – go recognize and go to the relevant R and then the table to understand how to comply – logical layout that is familiar to the industry.
- All of our programs are written in the format to comply with this format.
- Look at existing documentation and how it relates to current model – may be a burden to many to adjust to a new model without any clear payback.
- There will be a significant impact on documentation for any of the options. Yes, have an investment of time and resources in the existing CIP, but we should look at the next 3-5 year result. All of the models under consideration will require a major rewrite.
- Whatever we come up with needs to better than what we have no matter what the format – concern is that the substance is easy to understand and follow regardless of the format
- Are we going to stick with the h-m-l format? Be prepared if comments are universally against that format.
- Expect, like the past, that comments will be across the spectrum of support-nonsupport
- What is "better"? Building a house before we know what type of house we want.
- "Better" means concise, easy to understand and to implement.
- We identified about 90 security controls yesterday – if we have a new access control will we will have to add it in several places producing duplication?
- I assumed the twelve control groups were to be used to help distribute the new items into the current format – this would fix problems without creating new ones
- Stay with current structure or move to a functional model –satisfied with current model or ready to move on to something else?

- Discussed this issue before – writing the standards more like NIST is just one option – rewriting the current standards is not off the table.
- The issue is not NIST versus the current CIP structure. The question is does the current structure work or not. If not, what can we do to improve it? There may be resistance to change, but our task is to make the process better – "we can not keep the system as is and just move the deck chairs around."
- Difference between structure and organization – keep the current structure and the topical references? Same titles and thought processes?
- Yes the topics stay the same but the meat within may change – make the changes fit within that
- With CIP002 not sure fits with the old structures organization
- Where does the functional strawman fit? A new CIP-010 or in the existing CIP 003-009 structure?
- Preferably the latter

Option #1- Current CIP-003-009

Strengths

- Current structure allows industry to meet their respective needs.
- Industry understands system.
- Some industry concerned that proposed CIP002 is turning the world upside down – may need a hybrid to get the industry buy-in and acceptance

Weaknesses

- The current policy mixes enterprise wide policies and technical controls – confusion in implementation
- Number of TFEs and interpretation requests are indicative of some of the issues/problems with the current CIP.
- Focus on compliance versus performance assurance – some are focused solely on compliance and documentation, not measurable improvement in security.
- Core problem with current organization – topics are okay – but cannot understand and implement because we have moved away from commonly understood industry terms – key is in CIP005 and concept of perimeter and security enforcement mechanism.

Member Comments

- Are we here to fix the system or to change the terms of art?
- Keep the discussion on the structure – if task is to reword the current structure we could have done that long ago – are we tasked with redeveloping the standards for the industry or not
- Here to write a new standard or not?
- Not advocating keeping current structure as is – suggesting start with CIP 003-009 and reorganize as needed while keeping basic structure, can still have new Requirements – functional controls would fall into a table pointed to

- For existing structure option, will this allow us to still move things around? Yes, in particular to adjust for CIP 002. The table(s) still have to be tied to a standard.

Option #2- DHS standard

Strengths
- DHS leverages the work already done by the industry.

Weaknesses
- If move away from current structure, logistic issue of retiring all the current standards and start with CIP010 – for a couple of years there is potential for confusion – can keep current system and cross reference.

Member Comments
- Do we need to move away for question of documentation and talk about the technical difficulties of implementation?
- Where does electronic perimeter for a system begin and end? Left with an organization-by-organization determination of what and how to implement and hope you pass the audit – equipment out in the field what type of protection does it need – have to create things that do not exist today in order to comply for an audit.
- Cannot measure art – just because a group creates a strawman does not mean it is the right structure or just a pile of hay – security perimeter was created in 2002 at the request of FERC – our CIP-002 changes focus and sets the basis for h-m-l standard to bring focus of resources on the high.

Option #3- Strawman Approach

Strengths
- The strawman doesn't completely abandon the system understood by the industry – we identified 53 more controls yesterday – the strawman will accommodate the large number of new additions.
- The strawman offers a more logical grouping – not necessarily the final format –
- Group should not lose sight of the fact the strawman drafting group proposed and eleven-group structure.
- Talking about structure only, not content – the change shouldn't matter if it is easier to understand and implement – it is the substance not the structure that should matter.
- This format does leverage industries work and is not a radical change.

Weaknesses
- The more cross referencing you have, the greater opportunity for confusion – get caught in a repeating loop or circular logic –

Option #4- Prepare Requirements First, then Determine Format

The facilitators suggested an acceptability ranking of the three options. Several members suggested a fourth option which the Team tested.

Member Comments

- Can we right the requirements first, then find the model that fits them – I don't know what the right model is until I know what the parts are – a fourth option?
- Core issue is whether we stick with current structure or look for something different
- Prepare Requirements first?
- Don't know enough yet to know what structure we need
- Still too much unknown at this point – hopefully out of the drafting effort to develop requirements and controls will give us better idea of which format works best.
- Defer the format question until after drafting requirements. The Team will return to this by the end of March meeting

Prepare Requirements First, then Decide on Format

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	9	**6**	**0**	**1**	**3.3 of 4**

As a result of strong support for preparing the requirements first, the Team decided not to rank the acceptability of three options.

C. Subgroup Meetings and Reports

The Sub-groups met on Wednesday morning and early afternoon and then reported their initial results on the review of selecting candidate controls from the DHS catalogue. The Sub-groups met for a second time on Thursday morning and early afternoon to review security controls and begin exploring the drafting of requirements.

Prior to the second sub-team break-outs, the Team agreed on a sub-team format for collecting information with the following columns:

19. SDT Team Name
20. Section #
21. Title
22. NERC Security Guidance
23. NERC CIP-2
24. NIST SP 800-53
25. CSO 706 SDT Applicable
26. SDT Comments
27. Validated 706 SDT Applicable (Yes/No)
28. Existing CIP Requirement Cross Reference
29. FERC Order 706 References (Paragraph #s)
30. Requirement Definition

31. Controls- High
32. Controls- Medium
33. Controls- Low
34. Applicability- Transmission
35. Applicability- Generation
36. Applicability- Control Centers

1. Security Governance and Assessments *(Gerry Freese, Jon Stanford, Rich Kinas)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Note that the DHS doesn't call out "document" something such as CIP does
- Does in other areas
- In this area we may need to add "document" where appropriate
- Either cover globally as an opening statement or try to address where needed
- Cannot have implied documentation – must be called for in specific requirements – but should call for documentation where needed
- Do you have to document how you plan to document compliance?
- Assurance frameworks – federal standards referenced
- Excluded 2.2.5 and 2.2.6 – why?
- This has a federal slant to it – not that you shouldn't cover third parties but it is covered earlier in the standard – if write correctly then you can cover the third party situations in other areas
- DHS catalogue has a federal flavor and context
- Under NERC policy you cannot enforce on a third party except contractually
- Statute disallows you requiring a third party compliance – NERC cannot come in and obligate a vendor to follow requirements – NERC can only audit the registered entity
- Question mark by 2.7.1 – hard to put into CIP context and put into a requirement – the planning requirement in DIP is only implied –
- Concept of planning is good but coordinating between physical security and cyber security is very difficult
- Good placeholder item about how to deal with this one
- Know what is wrong but not sure how to fix it – strategic planning for security is a good idea, especially at a regional level – but need to be realistic, logical and not burdensome to individual entities – may fall outside these standards
- Can't write a standard to a functional model that does not exist yet – maybe CIP 10 is regional security coordination – make sure we are not creating work to create work – how do you craft requirement so they can be measured and audited for compliance? – but this idea into the parking lot for later consideration
- 2.17.4 – no? may want to parking lot "best practices" as a guidance document – agree it is not a requirement question

- If something is in the standards today then we were suppose to be reluctant to pull it out – is that true across the board – appears here that we may be pulling out items already in the standards
- Second to last column in the appendix has the CIP standards reference – need to gut check whether a few of these are included as topics rather than in intent of the requirement – needs a critical eye with as needed explanation as to why it is pulled out
- Vulnerability assessments included in several places – wording may not be the same – some of these no's should not be completely discounted – example is 2.17.2 and 2.18.4
- 2.18.11 and 2.1812 cover the issue
- risk management? Can only protect 90% - not writing controls to defeat your adversary – are we doing it justice if we throw it out
- reducing risk to an acceptable level to manage
- security control someone is looking for new threats and addressing them in a different way than we do today.
- That is part of risk management and risk decisions
- Is there a way to address risk management through the requirements? Put into the parking lot: a way to role risk management framework into the CIP requirements
- 2.18.6-10 are out
- 2.19.1??
- creating a whole new entity or beauracracy? – federal entities already have this – can we address this outside the federal context – parking lot: entity controls or common controls across entities
- there is a role for a forward looking plan – not sure how you audit or measure it
- can this be part of the assessment phase?
- 2.19.3??
- federal context this is identified – seems like a good idea – not sure how it applies to the private context; how it would look
- may have issues of measurement and enforcement – may be a good business practice but not in the requirements – same may be true of 2.19.2 –
- push back on "senior manager" from industry and this is even more prescriptive
- 2.19.5 already captured in CIP 002 – so it is a "no" here – it is here but only as a federal mandated response to specific legislation –

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Went through controls again but did not cross walk with CIP – will look back through CIP once have initial set
- Kept "organization" rather than "responsible entity"
- Reviewed requirement definitions – may have to adjust language to fit CIP

- 2.2.1-.3 pulled up into 2.1.1 language
- 2.2.4 belongs in the response section
- 2.7.1 – said no as is – 2.7.2 develop a security plan – not much changed from DHS – if we keep ESP then need to go back and reference here
- Did not include change to BES cyber system.
- Enterprise architecture? May not want that concept – the concept was a response to Federal law – left here until we determine if and how we want to address across other areas too
- the controls in this case are the requirements
- 2.7.10 – plan update
- May need to be prescriptive here using the table
- 2.17.1 – changed to NO and removed as too cumbersome – noted as a "?" in the first pass – not much benefit and anticipate huge push back from industry – difficult to monitor or test
- 2.18.5 – control system connections – difficult to take federal concept into the CIP/BES mind set – many vendors require a connection into your system to service their equipment – may need some assurance at both ends – should at a minimum document the relationship exists
- This is a mutual distrust, defend against friend and foe – that is where the concept of ESP comes in
- Opening a hole to a vendor
- Discussed as a team and pushed the issue over to security operations.
- 2.18.2 moved up above
- 2.191 captured in global policy
- 2.19.2 removed as too directive – may damage most organizations in terms of accountability
- 2.19.3 removed
- Figured out the first requirement – looked primarily at the DHS catalogue but making adjustments to language as needed
- Policy that addresses issues out of CIP002
- Assuming .1 requirements are being put into a policy section of CIP 003 – went through 2.1 and listed the policy and the sub-policy under it
- Also reviewed NIST language to see if it works in CIP context
- Illustrative example in 2.7.1 – document to explain a document? A policy that points to a program that may not exist?
- Thinking we may need to take this out – current words has a federal only context
- Do we change the CIP requirement?
- Look at 2.2.2 – high level policy set out in 2.2.1 – if leave this one in as a requirement may be adding layers of bureaucracy – this may be an opportunity to clarify, simplify and make it more implementable

- Eliminated some sub areas identified yesterday
- Tidy up and scope DHS language. Go back later and look at existing CIP- and drafts and lift all the ".1"s up.
- Instead of "Organization" will use Registered Entity (RE) consistently.
- The Sub-Team requested that Dave Norton join their team. Chair and Vice Chair also suggest checking with John Lim to see if he might join when he returns.

2. Personnel and Physical Security. *(Doug Johnson, Rob Antonishen, Kevin Sherlin).*

a. First Break Out- Identifying Candidate DHS Security Controls

- Covering DHS 2.8 Operations Security; 2.11 awareness training; 2.4 Physical security; 2.10 system maintenance; and 2.14 System integrity
- How should we pick up current CIP requirements that have no equivalency in this section? "Leadership" e.g. doesn't belong in CIP 003. How to ensure these get captured.
- "The designated manager" is a generic reference.
- Exceptions- CIP requirements- no explicit treatment of this in the DHS.
- Does this go in governance?
- 706 order- define- "parameters of exceptional circumstances" needs to go somewhere? Back in Governance?
- Factor in outstanding interpretations for current CIP standards.
- Reassessed the validity of the DHS judgment on CIP- couple dropped, with a couple back in.
- Some in other groups? E.g. ".1" policies
- Got to one requirement- personal screening. Looking to draft less on the how and more on the what.
- Principle: Wording of standards- similar wording in both- conceptually equivalent. Stick with old CIP wording where possible unless 706 requires otherwise.
- Principle- keep the detail level of the current CIP.
- Consistent with Access Control.
- Shortening up requirements.
- 2 ways to write requirement. The responsible entity shall have a program …consistent with state, federal. (consisting of placed somewhere else).
- Howard G:
- All go in the requirement, unless there are going to be differences between H/M/L and environments.
- FERC says improve the reliability standards.

- By adopting the standards, we said this is acceptable for reliability. For making less restrictive.
- E.g. if we were to scrap 7-year refresh. Or change to 10 years, we would need a compelling reason. Change to 5, i.e. strengthen it and you will be fine.
- FERC just approved TFE filing but requires a compliance filing. Within 90 days. Put those 2

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Started working on personnel security and training (2.3 DHS). Started with CIP and noted where changes made and suggested additions.
- They have some of the FERC order items in the mix.
- We will need to go into the determination high/med/low ahead.
- Need to get into the Physical security side. (2.4 DHS).
- 2.11- awareness training and training before access.
- Sub-team will get with the Access Control and Auditing Sub-Team.

3. Operations Security *(Jay Cribb, John Varnell, Jackie Collett & Jim Brenton)*

a. First Break Out- Identifying Candidate DHS Security Controls

The sub-team started with the following example to see what requirement drafting might entail (*E.g.*2.8.7)

1. The RE shall insure that all BES Cyber System component are within an Electronic Security Perimeter.
2. The RE shall manage the ESP gozintas and gozoutas (insert table to define "manage" at the different impact levels/environments).

E.g.

Ports /services enumation	H	M X	L X	CC/Gen/Tran
Strong Auth. For Remote Interactive Access	H	M X	L	

- Boundary protection 2.8.7
- 2 requirements. make sure everything in boundary and manage that boundary.
- What does "manage" mean at that level? Take sub Rs in 005 and put down left side of table.

Member Comments

- PH Defined ESP around crucial cyber assets- in CIP 002- boundary access control into and out of the cyber system.
- Why define a boundary? Need to know what is coming in going out.
- **2.8.7** talks about identifying a boundary.

- **I**s there a need of providing a glossary of new terms we should use as we write these requirements?
- If concepts roughly the same, use the "term"- Re-define to take out the CCA.
- CIP is tied around CCAs? Do CCAs have to be inside it? Boundary at DHS is generic. It isn't tied to asset, category or definition.
- If not ESP, (or use electronic security boundary) looking at this as more of a concept.
- Boundary "protection" is a function- critical cyber assets and a boundary around them, or perimeter.
- CIP tied to assets vs. federal concept of compliance. Problem with "electronic boundary" is that it constrains compliance.
- Think of "network boundaries"
- There is no standard in industry as to what an ESP is. Industry grappled with this one.

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- The Sub-team met with the Access Control and Auditing group to coordinate and clarify which sub-team would deal with the access control issues in security operations.
- R1 and R3. Controls 2.87
- Drafted 5 requirements and added rows to the chart.
- High level –general ideas for requirements.
- Sub-requirements in R1 are definitional matters. Sub-team started a list of definitions, e.g. access points defined.
- #2- needs to scope this one as it represents a whole new concept.
- Sub-team is reworking R1, 4 and 5. They are a mess today. The Sub-team will make more succinct.
- Security systems- access control, monitoring. Some are monitoring more than 1 system.
- Are there auditing issues in R4 and R5?
- Went through R1 and R3 in CIP 005 and came up with five requirements with all components within the ESP and all Access Points are identified
- Need much more definition to Electronic Security Perimeter
- Also Remote Interactive Access
- Systems within the ESP are part of the Cyber System (R1.4 and 1.5)
- Monitor and log all access through an ESP Access Point
- Caution – security monitoring systems may monitor or protect more than one BES cyber system
- 1.4 and 1.5 look like monitoring systems – may need to coordinate with Auditing sub team
- Add summary description to document proposed changes

- May want to build a related glossary – be sure we are using the terms consistently across all the sections

4. Recovery and Response *(Jeri Domingo Brewer, Jason Marshall, Joe Doetzl, Scott Rosenberger)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Validation of CIP and cross-reference and evaluate 706 whether there were paragraphs directed changes to these standards/requirements.
- "Continuity of operations" DHS- much broader.
- CIP- recovery and incidence of response. Overlap with other reliability standards.
- Clarify who and what this applies to
- Training in CIP 004 may take care of this training.
- Incident handling-look to FERC 706 paragraph.
- Looking at requirements next.

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Continuity of operations – part of critical business function practice –
- CIP 008 and 009 are straightforward
- Incident response: there are some elements regarding training, those pieces may need to remain in personnel training but overlap we need to discuss
- In the physical section there was a section on location of physical assets – does that fit more in your section?
- Much of the requirements are straightforward and will not require significant rewrites
- High impact- to low impact
- Federal government concept of "vital records" relates to continuity of service/operations. Requires more comprehensive planning than CIP.
- Incident response
- Training requirements- regarding recovery and response. Not clear whether these stay in this section vs. group responsible for training
- Physical section addresses choice of physical location of assets.
- Scott Rosenburger will take the lead from here on this section along with Joe Doetzl.

5. Access Control and Auditing *(Sharon Edwards, Phil Huff and Jeff Hoffman)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Assumed the table and decisions apply to high impact only
- "Yes" means we will look at it further, not necessarily adopt in whole
- Account Management- 2.15.3- side-by-side CIP and DHS comparison.
- E.g. deleted #9 DHS side.

- Cross-referenced to existing CIP language.
- This should be incorporated into CIP #7 "specifically authorizing and monitoring the use of guest/anonymous accounts.
- Helpful to see what Jay's team did.
- E.g. periodic review- line items that could be put into a table format.
- Got through 1 out of 15 controls on our plate. Time is needed for this.
- Separation of duties? Cannot be done in some cases
- Looking at separating administrative from security duties
- That is a best practice, and should not be a requirement subject to possible fines
- Original intent was to have two people to verify an action by separating or limiting the scope of respective roles, Turn into a recommended practice, not a requirement
- Need to go back through the items in gray – assumed they were already in the CIP, but need to review them further

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Sub-Team focused on understanding the process and walked through one in detail – then divided up the rest for further work
- Identified changes to CIP
- Concerned that the current language allows organizational approval rather than specific individual. However, that allows for different organizational structures.
- CIP says "designate" rather than "authorized" – the former is more rigorous
- If CIP is the master language – having trouble putting into a master spreadsheet designed to address DHS requirements
- Need to modify the table to note CIP language not covered by DHS catalogue – add a row to each family
- End of presentation-- governance question.
- Clarify the meaning of "appropriate approvals."
- This is hard issue in terms of DHS and CIP.
- In the Federal context, this is shown by testing. It is built into the system as a performance framework and life cycle maturity.
- CIP- granular language- is this a weak compensation for a more mature control?
- What happens to a documentation step?
- Approval by "Designated personnel"
- Separately requires a list of who are the authorizing individuals.

6. **Change Management System Lifecycle and Information Management.** *(Dave Revill, Keith Stouffer and Bill Winters)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Didn't get to 706 yet. Next task after cracking requirements language.
- Got through 1 family. 3 requirements left in. Removed 2-3 had yes on yesterday but on further review.
- 2.5.1 punted to the governance group.
- Requirement- policy 1.2.5.1, 2.5. 4, Acquisitions (dropped 252 and 253).
- E.g. 2.5.4 The organization develops security functional requirements specifications and documentation requirements for the BES cyber system acquisitions.

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- 5 families (12-15 in each family)
- Sub-team has got through 1st family.
- First 3 controls of 2nd family (maybe an overlap with maintenance)
- When equivalency- the harmonization exercise takes more time.
- Configuration and change management
- System life cycle (not much overlap)
- Information mgt.- tough family regardless-
- 2.5.7 User installed software. Said yes initially. Really turned out more about authorizing to install. Since this is already managed through configuration change management process approval, we changed this to No.
- DHS-less concern about saying things multiple times unlike CIP.
- 2.6.1-policy will be handled by the Governance Sub-Team.
- Baseline configuration. - Mitre report and mapping from DHS catalogue. Suggested including in CIPS. Sub-Team didn't agree with that.
- Control written.

D. Final Reflections on the Sub-Team Output

On Friday morning, following the sub-team reports, the Team offered reflections on the sub-team exercise.

- Where does spreadsheet end up – is it proof we considered or is it just and internal document – may need to be careful in the comments
- Initially this should be just an internal documentation of the Team's discussion and agreements.

- Suggest more is better since we do not know its future – unlikely to be filed with a regulator but not sure how much justification we need in a text formatted future filing – also may be circulated as email to + list which makes it virtually public
- Don't think I need to justify why a DHS does not fit in CIP – "considered" as requested.
- May want a little more detail than just "too cumbersome" for our own use a few months down the road.
- Denote and label this document as a "working draft."

IV. NEXT STEPS

On Friday morning following the Sub-Team reports, the facilitators presented and the Team reviewed and refined the next steps and assignments emerging from the meeting:

A. Next Steps- SDT

1. Revise the Strawman based on Tucker outcomes- Phil and circulate to SDT
2. Get the overall SDT schedule/work plan out ASAP consistent with adopted NERC schedule (Scott Mix and Bob Jones)
3. Members provide comments early next week on draft Webinar materials to Jay/Sharon(by Tuesday/Wed)
4. Members provide questions to Joe B for FERC/NERC consideration at Jan 28 meeting by Jan 26. Joe will send around info on phone link up etc. Members consider participating.
5. Feb 3 Webinar- members encouraged to participate. Jay and Sharon lead.
6. Draft Tucker Summary circulated to SDT by end of Jan.

B. Sub-Team Assignments

1. Sub-teams will request today or ASAP assistance from Howard, Scott or Joe in their meetings and set their meetings and coordinate with Joe
2. Get the sub team master schedule from next week to Austin out ASAP. NERC will help resource these in terms of ready talk. (Joe B coordinates)
3. Recovery and Response- Jeri will send to Scott R. draft and join the first conference call meeting.
4. Prepare progress reports and any key questions for presentation in Austin on Friday morning.

C. CIP 002-4 Review

1. 'Ugly Dump" of raw comments from Industry on February 9th or 10th to be sent to the team (Scott Mix).
2. Informal Industry Comments due by Close of Business Friday February 12, 2010.
3. Meeting in Phoenix. 1 p.m. Tues- Feb 16 (15 is holiday) through noon on Friday February 19.
4. Draft Compilation and organization of comments and to be sent out over weekend. Feb 13 or 14 (John Lim and Scott Mix).
5. Full and small group review of comments and consideration of changes to CIP 002-4.
6. Agreement on CIP 002 as revised for posting for 45 day at conclusion of Austin meeting.

D. Work plan and Schedule Review

Scott Mix presented a revised proposed schedule for CIP 002 and the security controls requirements *(See Appendix #5).* The Team liked the presentation in which the two efforts are put in parallel columns and shows the amount of work ahead.

E. FERC/NERC Workshop Questions
Phil Huff reviewed some questions that the Team discussed for FERC meeting next week including:

1) What expectations are there regarding coordination with the Smart Grid CSCTG (Cyber Security Coordination Task Group) product and how we use NIST SP 800-53/DHS Catalogue?
2) NIST SP 800-53 is an organizational risk management framework, which allows for tailoring and compensating controls. However, FERC Order 706 calls for extensive oversight for any exceptions. What are their thoughts on reconciling these seemingly conflicting objectives?
3) The process to make modifications to the Standards through a FERC Order is very resource intensive. Conversely, changes made prior to industry balloting are relatively cheap. Is it possible to have a process where the team can receive feedback from FERC prior to ballot?
4) To what degree can we remove or lessen prescriptive elements in the current CIP Standard where the risk reduction does not justify the consumption of industry resources?
5) Have we captured all of the directives from order 706 in the filing from December?

He noted this was a working list which will be circulated for members to suggest additions to in advance of the January 28 FERC/NERC workshop.

F. Sub-Team Organization and Next Steps
Joe Bucciero will be soliciting from each Sub-Team their meeting schedules to produce a master Sub-Team schedule from this meeting to Austin. He noted that Ready talk will be made available to the Sub-Teams so they can review and share documents.

The facilitators noted that each Sub-Team should plan on preparing and presenting short progress reports and key questions for presentation at the Austin meeting which will primarily focus on refining CIP-002-4 in response to industry comments. NERC will try to get Maureen Long to the Austin meeting on Thursday to be available to address the response and refinements of the CIP-002-4. The Team needs to reach agreement on CIP 002 as revised for posting for 45 day period.

Phil Huff on behalf of the SDT thanked Jeri Domingo Brewer for her leadership over the past 16 months. Ms. Brewer acknowledged the opportunity to get to know the SDT members and noted the honor of having worked with them to produce excellent and timely outcomes. She urged the Team to continue to build on the foundation of trust and collegiality to complete the task assigned by December 2010.

Mr. Huff then thanked Dave Revill for hosting the meeting and providing excellent support for this critical meeting.

The SDT adjourned at 12:30 p.m. on January 22, 2010. Several Sub-Teams continued to meet following lunch on Friday afternoon.

Appendix # 1— Meeting Agenda

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

Proposed Meeting Objectives/Outcomes

- Review the CSO 706 SDT 2010 Work plan
- Receive update on the CIP 002-4 filing and review process lessons learned
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan
- Review, discuss and test consensus for CIP guiding principles
- Review strawman documents, discuss and test consensus for CIP security controls approach, guidance, scope and applicability.
- Convene CIP Security Controls Drafting Groups
- Review Drafting Group Reports and Provide Feedback
- Agree on next steps and assignments

Draft Agenda

Tuesday **January 19, 2009**

1:00 p.m. Welcome and Opening Remarks- *Jeri Domingo-Brewer & Phil Huff*
Roll Call; NERC Antitrust Compliance Guidelines
Facilitator review and SDT acceptance of December 15-16, 2009 Little Rock SDT meeting summary
1:15 Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:20 Review of CSO 706 SDT Work plan- January-June, 2010- *Stu Langton*
1:40 Update on CIP 002 Filing- Process Lessons Learned- *Joe Bucciero*
2:00 Other Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
2:15 NERC Update on Implementing the CIP Communication Plan
2:30 Overview of Security Controls Strawman Documents and Drafting Group Process
3:00 Review, Rating and Consensus Testing of Principles
4:00 Review Strawman Security Controls Categories and Proposed Drafting Sub-Teams
4:30 Review and Consensus Testing of Sources for Controls
5:00 Review of Required Elements for Each Security Control
5:15 Member Drafting Sub-Teams Preference Survey
5:25 Review of Proposal for Wednesday Agenda and Drafting Groups
5:30 *Recess*

Wednesday **January 20, 2010**

8:00 Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:10 Review of CIP Security Controls Drafting Template- *Scott Mix and Howard Gugel, NERC*
8:45 Review and Agree on Proposal for Drafting Security Controls and Sub Team Members

10:00	Convene Organizational Meetings of SDT Cyber Security Controls Sub Teams
12:45	Reconvene SDT Cyber Security Controls Sub Teams
3:0	Sub Team Organizational Reports, Requests and Needs and Full Team Feedback
4:50	Review Assignments and Thursday Agenda
5:00	*Recess*

Thursday	**January 21, 2010**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15	Review any Drafting Group Requests/Needs
8:30	Reconvene SDT Cyber Security Controls Sub Teams
	Reconvene SDT Cyber Security Controls Sub Teams
3:00	Sub Team Reports and Full Team Feedback
4:50	Review Assignments and Friday Agenda
5:00	*Recess*

Friday	**January 22, 2010**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15	Review any Drafting Group Requests/Needs
8:30	Reconvene SDT Cyber Security Controls Sub Teams
12:30	Sub Team Reports and Full Team Feedback
2:30	Review and Agree on Next Steps for Developing Security Controls (CIP 003-009) and Work plan for February 2010 Meeting on CIP 002-4 Industry Comments
	Meeting Evaluation
3:00	*Adjourn*

Appendix # 2 Attendees List

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (Thurs)
2. Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
3. Jim Brenton (Wed-Fri.)	ERCOT
4. Jackie Collett	Manitoba Hydro (Wed/Thurs)
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Sharon Edwards	Duke Energy
7. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
8. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
9. Doug Johnson	Exelon Corporation – Commonwealth Edison
10. David S. Revill	Georgia Transmission Corporation
11. Jonathan Stanford	Bonneville Power Administration
12.Keith Stouffer	National Institute of Standards & Technology
13. John D. Varnell	Technology Director, Tenaska Power Services Co. (Wed. Thurs)
Roger Lampilla	NERC
Scott Mix	NERC
Howard Gugel	NERC
Gerry Adamski (Tues)	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 Ready Talk and Phone

14. Joe Doetzl (Wed)	Manager, Information Security, Kansas City Pwr. & Light Co. (Thurs.)
15. Frank Kim (Thurs)	Ontario Hydro
16. Rich Kinas (Wed/Thurs)	Orlando Utilities Commission (Wed.)
17. David Norton	Entergy (Wed.
18. Scott Rosenberger (Wed)	Luminant Energy
19. Kevin Sherlin (Tues-Fri)	Sacramento Municipal Utility District (Wed. Thurs.)
20. William Winters (Wed-Thurs)	Arizona Public Service, Inc.

SDT Members Unable to Attend

1. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY

Others Attending in Person

Jeff Hoffman	USBR
John Falsey	EMMT
Jason Marshall	Midwest ISO

David Van Winkle	GTC

Others Attending via WebEx and Phone

Rob Hardiman	Southern Company Transmission
Joseph Baxter	AECI
Justin Kelly	FERC
Justin Kelly	FERC
Michael Toecker	Burns and MacDonald Engineering
Bill Glynn	Westar Energy
Sam Merrell	Cert
Rob Wotherspoon	Orlando Utility Commission
Michael Fischette	LBWL
Laurel Moll	Orlando Utility Commission

Appendix #3

Meeting Evaluation Feedback for Inclusion in Team Meeting Summary

The SDT members used the following 0-to-10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree. This reflects 12 member responses.

1. Please assess the overall meeting.

8.00 The agenda packet was very useful.
8.14 The Ready Talk document display and the audio were effective
9.40 The quality of the meeting facility was good.
8.50 The objectives for the meeting were stated at the outset.
8.33 Overall, the objectives of the meeting were fully achieved.

Was each of the following meeting objectives fully achieved?

8.50 Review the CSO 706 SDT 2010 Work plan
7.88 Receive update on the CIP 002-4 filing and review process lessons learned
8.71 Receive updates on other related cyber security initiatives
8.00 Receive a NERC update on implementing the CIP Communication Plan
8.63 Review, discuss and test consensus for CIP drafting principles
8.50 Review straw man documents, discuss and test consensus for CIP security controls approach, including drafting sub-teams, sources for controls and required elements for each security control.
9.50 Convene CIP Security Controls Sub-Teams
9.43 Review Sub-Team Reports and Provide Feedback
8.75 Agree on next steps and assignments

2. Please tell us how well you believe the Team engaged in the meeting.

7.63 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
8.89 The Facilitators made sure the concerns of all members were heard.
8.63 The Facilitators made sure the concerns of all participants were heard.
7.63 The Facilitators helped clarify and summarize issues.
7.25 The Facilitators helped members build consensus.
7.63 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

7.44 Overall, I am very satisfied with the results of the meeting.
7.80 Overall, the design of the meeting agenda was effective.
8.70 I was very satisfied with the services provided by the Facilitators.
7.90 I am satisfied with the outcome of the meeting.
6.89 I am satisfied with the progress we are making as a Team.
8.80 I know what the next steps following this meeting will be.
8.80 I know who is responsible for the next steps.

4. Other comments (use other side)

What did we achieve?

- We decided not to meet the schedule by not saying we will do other stuff besides fix existing structure.

What are our biggest challenges going forward?

- Timetable.
- Time/resources.

What suggestions do you have for making the Team more productive?

- Get the members to express their concerns in a more productive manner.
- Read out loud FERC ORDER 706!

Appendix # 4 — 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 Subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

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

III. Activities That Are Permitted

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

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

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

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

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

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

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

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

APPENDIX # 5
MEETING SCHEDULE
JANUARY –DECEMBER 2010

Preliminary, Draft, Unofficial Schedule for CIP-002-4

CIP-002 Task	CIP 2 Milestone Date	Week-of	Date	CIP-003 -- CIP-009 Task
		1/18/10		SDT Meeting - Work on requirement language
		1/25/10		sub-team meetings
		2/1/10		sub-team meetings
Informal Comment Period closes	2/12/10	2/8/10		sub-team meetings
SDT Meeting - React to comments		2/15/10		
Post for 45-day formal comment; form ballot pool	2/25/10	2/22/10		sub-team meetings
		3/1/10		sub-team meetings
		3/8/10		SDT Meeting - Work on requirements
		3/15/10		post initial unofficial draft (aid in CIP-002 ballot process)
		3/22/10		sub-team meetings
Initial Ballot start	4/2/10	3/29/10		sub-team meetings
		4/5/10		sub-team meetings
Initial ballot close; SDT Meeting - respond to comments	4/12/10	4/12/10		
		4/19/10		sub-team meetings
Recirc Ballot start	4/30/10	4/26/10		sub-team meetings
		5/3/10		sub-team meetings
Recirc ballot close; SDT meeting - respond to comments	5/10/10	5/10/10		
Re-recirc ballot start	5/16/10	5/17/10		sub-team meetings
Re-recirc ballot close; BoT Approval	5/25/10	5/24/10		sub-team meetings
File with Regulators	5/31/10	5/31/10		sub-team meetings
		6/7/10		SDT Meeting - Work on requirements
		6/14/10		
		6/21/10		
		6/28/10		
		7/5/10		
		7/12/10		SDT Meeting
		7/19/10		
		7/26/10		
		8/2/10		

OCTOBER 2008–JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.

- January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
- January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

March 2–April 1, 2009 — 30-day Pre Ballot

Mid-March — NERC posts TFE draft Rules of Procedure for industry comment

March 30, 2009 — WebEx meeting(s) White Paper Drafting Team

April 1–10 — NERC Balloting on Version 2 Products

April 6, 2009 — WebEx meeting — White Paper Drafting Team

April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call

April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx

April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.

June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada
SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010
September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)
- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002-4 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002-4 for industry review and comment.
- Agree on next steps and 2010 Work plan and schedule
- December 28, 2009 SDT Conference Call on CIP 002-4
- December 30, 2009 SDT Leadership Call- Security Controls Survey Draft

Appendix #6
MASTER SDT SURVEY RESPONSES FOR DEVELOPMENT OF CYBER SECURITY CONTROLS
(Updated Jan 12 2010)

16 SDT Member Respondents: **Rob Antonishen, Jim Brenton, Jackie Collett, Jay Cribb, Joe Doetzl, Sharon Edwards, Phil Huff, Doug Johnson, John Lim, Dave Norton, Chris Peters, Dave Revill, Scott Rosenberger, Kevin Sherlin, John Varnell, William Winters**

SDT Members Unable/No Response: Jeri Domingo-Brewer, Gerald Freese, Frank Kim, Rich Kina; Jonathan Stanford, Keith Stouffer
Industry Respondents: Thomas M. Overman, Boeing

NOTES:
1. This survey, developed by the SDT Chair and Vice Chairs over the holidays, is divided into 4 sections: Guiding Principles; Security Control Approaches; Security Control Guidance; and Security Control Scope/Documents and Applicability. It was sent to the Team on Wednesday, December 30 with a deadline of noon, January 5.
2. Within each section the statements/proposals are listed from "most acceptable" to "less acceptable based on an averaging of the member "acceptability ranks for each statement. Member comments and pros/cons are also included.
3. A SDT Sub-Team, made up of interested SDT member volunteers, will take these survey results following the January 6 SDT conference call and create a strawman document for review by the full team in advance of the in advance of the Jan 19-22 SDT meeting in Tucker, Georgia.

Interest in participating in a temporary SDT drafting group and able to commit to drafting documents and participating in up to two conference call meetings between January 6 and January 15 to produce draft strawman proposals for the development of security controls that will be reviewed by the SDT in Tucker?

Yes: **Jim Brenton, Jay Cribb, Joe Doetzl, Sharon Edwards, Phil Huff, Doug Johnson, Kevin Sherlin, John Varnell,**

No: John Lim *(Not available most of January)* Dave Revill, *(I would like to, but I can't make the time commitment necessary during those 2 weeks. I would like to participate as some sort of alternate when time allows if possible.)* Rob Antonishen (*Sorry – just don't have the time…I'm even getting pushback to 4 day meetings…)* Chris Peters, Scott Rosenberger (Team, I am interested but am sorry that I will not be able to dedicate the additional time with the current job requirements. I am working to get the appropriate staff added to lighten this load but that will take some time. Thanks**),** Jackie Collett, Dave Norton, William Winters

Yes- Thomas M. Overman, Boeing

SECTION 1: DRAFT STRAWMAN GUIDING PRINCIPLES FOR THE DEVELOPMENT OF SECURITY CONTROLS

A. **In developing security controls, the SDT will seek to minimize overlap, duplication, and reduce complexity of the requirements and controls.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	12	**3**	**0**	**0**	**3.8**

Comments:

- Common sense.
- **It may be necessary to duplicate some items/sections to provide simplicity.**
- Who can argue against that? It's a source of much confusion in the current set of standards where all sorts of related things are split across standards and have different implementation plans and timeframes. We've got to stay away from that.

B. **In developing security controls, the SDT will document the security objective to be achieved for each security control to aid in future interpretations.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	10	**6**	**0**	**0**	**3.6**

Comments:

- The emphasis should be on documenting the appropriate controls. If the SDT is diverting into documenting all of these items, it may take time away from the primary objective of documenting the controls. Some of these, i.e., reduction of risk to the BES functions, if done, may be follow-up items. Care should be taken to ensure that identifying and documenting appropriate controls is the priority.
- I don't disagree with this. However, I believe that if the security objective isn't already clear from the language in the requirement, then perhaps we didn't do a very good job writing the requirement.
- *THIS WILL ALSO HELP THE TEAM TO MEASURE THE VALIDITY OF THE OBJECTIVE AND WHETHER OR NOT THE SECURITY CONTROL ACHIEVES IT.*
- *This would be very nice to have though not essential. We should use a standardized framework if pursued to aid in standardized objectives (such as ISO,NIST)*
- If we are too narrow in defining our security objectives, we may not be able to provide enough flexibility for the future security landscape.
- This seems mandatory – isn't this what a requirement is all about? If we are doing 'what' and now 'how' standards then this is basic. It seems that ALL we would state is the security objective to be achieved and going beyond that means we have dropped into 'how' standards.

C. **In developing security controls, the SDT will document how each security control (and enhancement) reduces the risk to the BES functions appropriate to the impact categorization.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	9	**5**	**1**	**0**	**3.5**

Comments:

- The emphasis should be on documenting the appropriate controls. If the SDT is diverting into documenting all of these items, it may take time away from the primary objective of documenting the controls. Some of these, i.e., reduction of risk to the BES functions, if done, may be follow-up items. Care should be taken to ensure that identifying and documenting appropriate controls is the priority.
- I am not sure how this will benefit us in the long run. I think our time would be better spent writing guidance for controls.
- Again, I have the same reservations as for question A. Any such documentation will have to exist outside the standard as (it is my understanding) that standards should not provide the rationalization, only the requirements and measures.
- *THIS MAY BE DIFFICULT TO DOCUMENT, BUT WE SHOULD AT LEAST AVOID INCORPORATING CONTROLS SIMPLY BECAUSE THEY ARE LISTED SOMEWHERE ELSE.*
- *Another nice to have and should be tied to standardized objectives*
- Not sure how we will do this and what value it will provide, while not releasing potential sensitive information.
- I think this goes to Gerry Cauley's remarks that he's made several times recently – how every requirement ought to be tied back to how it improves or preserves BES reliability. If we can't do this, then we have no business making it a requirement in a mandatory BES Reliability standard. If we can't do this, then we are doing security for security's sake and we've taken our eyes off the goal.

D. **In developing security controls, the SDT will consider how compliance can be demonstrated.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	11	**2**	**3**	**0**	**3.5**

Comments:

- I agree that we should "consider" how compliance can be demonstrated, but that is not our primary goal. This is only acceptable if time allows. We may not have time to document compliance measurement. Some other items such as ensuring that appropriate controls are identified are more important as a responsibility of the drafting team.
- The purpose of the standard is to provide better reliability through proper cyber security posture. I am strongly opposed with any type of standard/controls that will eventually lead to a "checkbox" audit mentality. A proper understanding of the intent of the controls should lead to an adequate understanding on how to achieve compliance, while still providing the flexibility necessary in the IT security field to keep the standard in line with current technologies and practices.
- *I AGREE COMPLIANCE SHOULD BE CONSIDERED, BUT A FRAMEWORK THAT ALLOWS COST-EFFECTIVE RISK-REDUCTION IS MORE IMPORTANT THAN ONE THAT EASILY DEMONSTRATES COMPLIANCE.*
- *How will this be addressed in light of reports of auditors not using the measures section of the standard?*
- Since these are mandatory and enforceable standards, this is mandatory for us. We MUST have it clear in the standard with bright lines how an entity knows they are compliant with the requirement and how they will be measured. Anything less is unacceptable in this environment. These are not 'suggestions' or 'good ideas', these are mandatory, auditable, and enforceable. They must have clarity in this area.

E. **In developing security controls, the SDT will set forth and document clear rationales for changes made to the current Version 3 CIP 003-009 and how it protects current investments in security.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	7	**8**	**1**	**0**	**3.4**

Comments:

- The emphasis should be on documenting the appropriate controls. If the SDT is diverting into documenting all of these items, it may take time away from the primary objective of documenting the controls. Some of these, i.e., reduction of risk to the BES functions, if done, may be follow-up items. Care should be taken to ensure that identifying and documenting appropriate controls is the priority.
- I don't disagree with doing this. However, I believe that it is not our burden to provide rationalization for every change that is made to the standards. I believe that it is already well documented that changes are necessary
- Pertaining to the development of security controls any revised CIP 003-009 will, in my opinion, be a significant rewrite of the current (version 3) standard. I am concerned about the effort that will be incurred by any direction that requires either rationalization or justification of any changes or deviations from the current standard.
- *We will have to address the requirements of order 706 as well and should seek to clarify when a change is driven from this order vs. our attempt to make things better*
- While I agree that the industry needs to understand how their previous efforts are not wasted, this effort should not significantly consume our time and effort to get the standards finished.
- If timeframe is such a crucial issue, we may not have time for this. I expect that the changes to current requirements would either provide needed flexibility based on environment (field vs. data center, etc) or go beyond a current weak requirement – neither of which would need a lot of documentation of how it protects current investments in security. I don't see us doing anything that tears down the 'Security 101' that has been built with the current CIP standards.

SDT MEMBER COMMENTS

- I agree with many of the items above, but I'm not sure we should really focus on those as being our *principles*. Several of them seem to be more task-oriented than truly fundamental principles that we should fall back on in the drafting of our security controls.
- *Fundamentally I believe these principles should be in place for the development of CIP3-CIP9V4+, though I am not sure there is time to include all this in the draft strawman if the time target is for the Jan meeting,*

OTHER SUGGESTED DRAFT GUIDING PRINCIPLES

- In developing security controls, the SDT will seek to eliminate the necessity for Technical Feasibility Exceptions (TFE's) though proper development of controls and defining appropriate applicability of those controls.
- In developing security controls, the SDT will seek to eliminate or at least GREATLY reduce the need for a TFE process.

  Comments: We should never write a technically infeasible requirement. That is an oxymoron. They should all be scoped to feasible situations only.
- In developing security controls, the SDT will seek to reduce the compliance documentation and audit burden on the lower impact systems.

  Comments: If the industry has to focus much if not most of its resources on tracking and documenting compliance on the vastly higher quantity lower impact assets, we will have harmed security and BES reliability. The entire point of CIP-002 and classifying impact is so that we can FOCUS on the higher impact systems.

OTHER COMMENTS

Thomas M. Overman, Boeing

First make a distinction between Requirements and Controls. Some overlapping controls are OK (even good), but conflicting requirements are not good. The CIP is likely to remain the only Cyber Security Standard with regulatory authority. Therefore it may be necessary for the CIP to take a lead, or possibly to have requirements contrary to Cyber Security documents which do not have the same regulatory authority. The CIP must address known conflicts if any must remain.

Additional Principles

- In developing security controls, the SDT must draft threat vectors against which certification and accreditation must be judged.
- The SDT seek to minimize overlap, duplication, and reduce complexity of the requirements and controls.
- There may have to be a classified annex to address threat scenarios from a national perspective.

SECTION 2: DRAFT STRAWMAN SECURITY CONTROL APPROACHES

This section lists possible approaches in starting to develop the security controls. This will guide the team's decisions on how to divide into sub-teams and which security control catalogue to begin with.

A. Begin with the current CIP-003 to 009 requirements review and document the applicable Order 706 directives and review any new ways to combine and select those NIST SP 800-53 controls that should be used in a new CIP set of controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Industry is familiar with current organization	• Requirements may require significant overhaul.
• Preserves investment in compliance management frameworks (significant)	• We may end up with a product similar to past CIP.
• Preserves investment in investments in current controls	• 800-53 not measurable for penalties
• Utilizes industry effort to date.	• Highly defined controls give a black hat a list of things not to do.
• Leverages existing approved standards	• Very time consuming with little value
• Meet objectives of FERC Order 706	• Possibility of missing areas that are currently not addressed.
• Finite target	• **Personally, I'd like to see 006 be removed from the "cyber" set and migrated to a new (CIP-010?) standard that would address requirements for ALL BES assets, regardless of their cyber nature. This is not**
• Addresses the Order 706 in a concrete, easy to demonstrate method.	
• Maintaining the current structure provides a clear path for	

utilities to migrate to a new standard. • Potentially allows for maximum reuse of efforts by the industry • Will be seen as evolutionary rather than revolutionary. • Aligns with 706 intent • Simplifies CIP document structure • Organized CIP Standards into Control families • *Preserves current investment possibly* • *Identified changes as required by FERC* • Starts with something the entire team is familiar with (CIP Standards). • Order 706 directives apply directly to CIPs • Meets overall principle of preserving CIP V1-3 investment • Industry familiarity • Provides a roadmap for the industry from the current controls to the new controls • Provides a cross reference to Order 706 to ensure everything is addressed • Builds on previous work • Helps focus on Order 706	**inconsistent as the current CIP-001 in Sabotage Reporting is not cyber in nature.** • Significant time and resource commitments • *May not provide a holistic and new approach* • *Easier for industry to understand* • Many current requirements need major overhaul. • May be limited by NIST 800-53 • May be seen as more of the same

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	7	**7**	**2**	**0**

Avg. =3.3

Other Comments- Thomas M. Overman, Boeing

- Pros- Strengths= Good starting approach to phase into the more rigorous controls. Allows evolving and refining requirements rather than taking an entirely new approach (which would cause unnecessary industry churn.
  Cons- Weaknesses=CIP should also reference and synchronize with NIST 800-82 (Industrial Control System Security)
  In general, NERC CIP should address not only security processes/procedures, but also high-level technical requirements (without dictating technical solutions).

B. Begin with the current CIP-003 to 009 requirements divided into the security functions presented by the NERC Cyber Security Standards Education Team in 2006[1], review and document the applicable Order 706 directives, and review any new ways to combine and select those NIST SP 800-53 controls that should be used in a new CIP set of controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Used as a training concept. • N/A • This is going to occur somewhat anyway as we compare the current requirements to the NIST control families. • I am familiar with SET functions and support • Grouped into logical security functions similar to NIST 800-53, but in a way that the industry is familiar with. • Easier to incorporate 800-53 controls and prevent cross-references between Standards (or control families) • *I'm sure there are some* • Starts with something the entire team is familiar with (CIP Standards). • Could help eliminate overlap of requirements • Could better group requirements	• Security functions in training has no industry vetting • Not a recognized standard framework • Significant overlap with more recognized standards • I am not specifically familiar with the "security functions presented by the NERC CS Education Team in 2006…" • Would take some education for the team to understand exactly what rely on this NERC material means. • 800-53 not measurable for penalties • Highly defined controls give a black hat a list of things not to do • Time? • Can not comment as I am not familiar with this material • Don't understand the difference between A and B • *More difficult for the industry to understand*

[1] 2006 Cyber Security Standards Workshop Training Materials (Not Available on the NERC Website)

			• Unable to comment on the security function model – not available • Document not available. Can't rank this one • I do not personally know what the security functions presented were and do not have a copy to work from • Lack of familiarity with referenced work	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	2	**6**	**6**(Education)	**0**

Avg. =2.7

C. Begin with the current NIST 800-53 publication, incorporate the current CIP-003 to 009 Standard, and review and document the applicable Order 706 directives.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Comprehensive (though not entirely applicable) • Familiar to Federal agencies • Satisfies congressional agenda to utilize NIST approach • Best solution to meet FERC Order 706 • Current NIST 800-53 would provide a solid template to develop the standard from. • Will provide a mature model that should ensure covering all required areas • *Standards based* • Existing set of security controls • NIST controls written at what seems an appropriate level for broad applicability • Politically correct answer (Congress, etc) • Based on a known (800-53) body of work	• A large number of non-applicable requirements • Too general for application to Control Systems • Not enforceable in the current compliance model • This implies that everything in NIST 800-53 will become part of future NERC Cyber Security standards. I did not think the team had agreed to this concept. • 800-53 not measurable for penalties • Highly defined controls give a black hat a list of things not to do • May end up requiring the most amount of modifications to entities existing CIP programs • Deviating from the current structure of the CIP standards will make it difficult, timely and costly for utilities to migrate to a new standard. • May be seen as "throwing out the baby with the bath water" by the Industry, • While this effort would demonstrate adherence to the 706 Order, a significant restructure will undoubtedly introduce NEW areas that FERC will have issue with, and may result in a new Order as significant as the current 706 Order. • The NIST standard is not designed as an audit/enforcement standard, and as such may not be the best style to use for a reliability standard • This is a massive undertaking that the SDT is not organized to achieve. • Several controls assume an enterprise security architecture which would be difficult to demonstrate in the NERC compliance program. • *Does not preserve current investment* • Not all team members are familiar with 800-53 (learning curve) • Industry unfamiliar with 800-53 • Would make it more complicated for the industry to follow the changes • Might not be as clear how we could leverage existing security implementations

			• Applicability to industrial control systems	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	4	**3**	**6**	**2**

Avg. =2.6

Other

- As the Lead for the "Controls" sub group and a person familiar with NIST, does Keith have a recommended approach?
- The controls like in 800-53 should be a guideline not in the stander. This will make it where the auditors will allow new technology. NIST 800-53 ties us to today's technology only.
- *I find any of these approaches acceptable. I can't identify any pros/cons that have not already been submitted. I believe that A and B should be done in combination ensure that in the development of controls we have taken in to account what the ramifications are with respect to what the industry has already been taught and developed and ensure the documented 706 issues are all addressed.*
- *As we extend beyond the initial strawman, in addition to 800-53, I believe we should use the controls based standards referenced in section 3 as additional reference material since these may provide better verbiage and/or insight in the development of CIP Controls which need to be crafted as measurable standards.*

Other Approaches- Thomas M. Overman, Boeing

A. Defense Information Assurance Certification and Accreditation Process (DIACAP) provides a robust C&A guideline. As the Grid is a national asset, subject to attack by sophisticated state-sponsored adversaries, grid security should reference guidelines designed for such an environment. DIACAP is one such example.

B. Assess the risks (insiders, and external attackers, script kiddies to terrorists to organized crime to state-sponsored intelligence services). Two phases: Near term risk mitigation (procedural, some technical) vs. long term architectural and systemic approach.

SECTION 3: DRAFT STRAWMAN SECURITY CONTROL GUIDANCE

This section lists documents for the team to consider when drafting security controls (in addition to previous versions of CIP, FERC Order 706 and NIST 800-53). Although individuals or sub-teams may consider any guidance when drafting controls, the proposal would be to use these documents as a major influence and reference them in communication from the team.

A. Consider the DHS Catalog of Control Systems Security Recommendations for Standards Developers[2] in the development of security controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Control system centric • Is a good source for testing of completeness • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Comprehensive set of requirements • Supplemental Guidance wording provides useful wordage that would be used in explaining/justifying controls…but • This is being used to develop the Smart Grid Cyber Security Standards. We will immediately be compared with this effort anyway.	• Not meant for compliance monitoring • Time consuming – Do we have time and resources to research all of these documents • Too specific and will give a black hat a road map. • Too comprehensive – goes well beyond the existing CIP standard, in areas such as environmental control, supply chain requirements and strategic planning. • Supplemental guidance wording is necessary for understanding, but does not fit with the current NERC standard framework. • *Not as familiar*

[2] http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf

• Control System specific • Focused on control systems • Very detailed			• Many controls are more appropriately directed at control system vendors, not end users of purchased turnkey systems. • Has a lot of good ideas, but things that should not be mandatory requirements (honey pots, etc)	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	5	**6**	**4**	**0**

Avg. =3.1

B. Consider the SANS 20 Critical Security Controls[3] in the development of security controls.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• Well known in cyber security circles • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Common sense and needed • As reasonable list as any (based on a cursory review) • Technical focused • Offensive in nature • This is aimed directly at addressing system security. It provides a starting point to prioritizing controls on the basis of risk. • A review wouldn't hurt to make sure we have them covered at the end. • Good starting point			• Too general • Not control system specific • Not intended for compliance • Time consuming – Do we have time and resources to research all of these documents? • Not specific enough to control systems • Somewhat motherhood (based on a cursory review) • New Standard that some may not have had experience implementing • *Not as familiar* • Not control system specific, general IT specific • No surprises in a 'Top 20' – covers the basics. • Should already be included in other larger control frameworks. • High level document • Not focused on industrial control systems	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	5	**5**	**4**	

Avg. =3.0

C. Consider the ISO/IEC 27001 & 27002[4] Standards in the development of security controls.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• Well known and comprehensive framework and controls • Recognized international standards organization • Internationally accepted • Better suited to be used as a reference for completeness • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Common sense • Mature Standard • Concise • Internationally recognized			• Not specific to control systems • Not structured for compliance monitoring, more structured for certification • Time consuming – Do we have time and resources to research all of these documents • Have not read! • No access, will not comment or rank • Non-open, proprietary, for purchase only standards. • Generic IT security standard, not control system specific • If we are going to base on generic standards, let's just do NIST and be done with it. Our goal is to write BES Reliability focused standards, not reinvent yet another generic IT Security standard.	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*

[3] http://www.sans.org/critical-security-controls/cag.pdf
[4] http://www.27000.org/ (for purchase)

	4	**5**	**4**	**0**

Avg. =3.0

D. Consider the ISA 99[5] Standard in the development of security controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Industrial systems centric • ISA well accepted in industrial environments • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Mature Standard • *Matches my corporate program* • *Familiar to many*	• Not well defined • In development • Not structured for enforcement • Time consuming – Do we have time and resources to research all of these documents • Too specific and will give a black hat a road map. • No access, will not comment or rank • Could be too technical • Non-open, proprietary, for purchase only standards

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	2	**8**	**3**	**0**

Avg. =2.9

GUIDANCE DOCUMENTS COMMENTS

- In order to develop a complete set of controls, all of the aforementioned Standards should be considered with the caveat that NERC CIP/NIST 800-53 serve as the baseline and SANS, ISO, DHS, and ISA-99 provide supplemental or amplifying guidance.
- Does the team have enough time to consider many other security controls guidance?

SECTION 4: DRAFT STRAWMAN SECURITY CONTROL SCOPE AND APPLICABILITY

This section lists several methods for applying reasonable and appropriate security controls.

A. Consider applicability of requirements for differing environments for Generation, Transmission and Control Centers.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Significant increase in clarity of application and relevance of requirement • Support from stakeholders • Better compliance monitoring • We need targeted controls. • The lack of applicable requirements is one of the industry's major criticisms of existing CIP. • This is crucial to the success of our standards. • Takes into account operational realities • Is the only real justification for writing our own controls versus wholesale adoption of other control frameworks? • We need separate controls of each of the three environment • Might be simple for participants. • Value in a separation for "Control Centers" for entities that don't actually control any "big iron", NOT SCADA master type control centers. • Each environment is distinctly unique • Could reduce ambiguity for industry • *Addresses the differences specifically*	• Increases complexity of the requirement set as a whole • Increases the volume of requirements • Requires specific expertise in targeted environments of generation, transmission and control centers. • Targeting the approach will probably take longer. • It will make the quasi-governmental utilities mad. • Time consuming • This separation is a red herring. Of more value is the nature of the cyber environment and equipment (i.e. embedded single purpose microprocessor based devices vs. PC's versus severs, etc). • Significant level of effort • Requires in depth knowledge of each environment that may not be present on the SDT • Difficult to maintain • Need to examine further to determine if the controls we develop truly apply differently to different operating environments. • *More complex*

[5] http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821 (for purchase)

• *Allows greater focus on more critical areas* • Addresses 'one size fits all' flaw • Allows entities to do what makes sense in varying risk environments • Could help provide real examples for the industry	• May need a rename; 'Transmission' is not descriptive of what we're really talking about – we are talking about substation environments, or plant environments, or data center environments.

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	6	**5**	**2**	**0**

Avg. =3.2

A1. Establish the applicability of each environment (generation, transmission, and control centers) within each requirement.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Single catalog • All in one place • Allows an entity to focus on what is applicable to them. • Only if we use the existing 003 through 009 structure • This may save the SDT some time in writing the requirements. • May ultimately reduce documentation required by the entity. • Easier to maintain • Simplifies the management of the standard. • Easier for entities with more than one type of facility. • Easier to maintain by having a consolidated standard • This would be easier for the industry to read and comprehend. • *Simpler.* • A requirement is stated once in the standard	• Makes requirements complex • Difficult to draft • May require drastically different requirement formatting • May be confusing • Difficult to follow applicability for a specific entity of a certain type • *May not address specific differences* • Could make for huge, confusing requirements with numerous caveats. • All entities will have to search to find what applies to them • Could be out of date very quickly and lack flexibility with the ever changing cyber world • Difficult to follow •

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	3	**8**	**3**	**1**

Avg. =3.0

A2. Group all requirements for each environment of generation, transmission, and control centers, separately.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Clear set of requirements for each group • Ease of application for functional entities • Each set is simpler (i.e. requirements in each set are simpler) • May provide greater clarity. • Allows one entity to focus on the types of assets they own • Typically, different departments will be handling implementation at substations vs. plants vs. control centers, so this may ultimately improve readability of the requirements. • We need separate controls of each of the three environment • Simpler to follow • Lets entities focus on just what they need to do rather than having their requirements strung out and hard to find over an	• Increases overall volume of the standards • Duplication of requirements in each set • Increase work for responsible entities which are integrated. • Creates redundancy. • May create additional work for SDT. • This should be by functional model and BES function. • Have to make three updates for common items • Redundancy in the standard itself. • In the future, a single change could require multiple edits. • Difficult to maintain • The same requirement could appear in multiple places. • Might cause some redundancy for entities having more than one environment

entire catalog of controls. • Matches most organizational structures so each can be given their piece to implement. • Separated by function	• Would probably cause redundancy in the standards which could confuse the industry and auditors • May miss opportunity for common solutions

Acceptability Ranking Scale	***4** = acceptable**,** I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	4	**8**	**2**	**0**

Avg. =3.1

B. Consider differing vulnerability and threat (risks) in the design of requirements. Use differing levels of application (e.g. basic, enhanced).

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Reflect practical realities • Great philosophy • Proper risk assessments are the cornerstone of a sound security policy. • *Not sure (no rank)* • I think this is mandatory. A completely standalone non-networked system vs. a networked system should have differing requirements • This could be used to limit controls applied to cyber devices that have no external connectivity •	• Increases complexity • May change over time • Confusing to write. • The approach lacks clarity and may change rapidly. • Cyber vulnerability and threat is not risk to the BES • Not sure we can make this paradigm shift with our current schedule. • FERC may not accept any acceptance of risk, especially given the current national security posture. • If we consider different vulnerabilities and threats as a basis for applicability, then we assume a demonstrable risk management framework. • *Not sure (no rank)* • We have to figure out how to handle inherited security via compensating controls, but this is a must do anyway. • Requires significant detail and is complex

Acceptability Ranking Scale	***4** = acceptable**,** I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	5	**3**	**5**	**0**

Avg. =3.0

C. Consider differing applications of requirements for general purpose software operating environments and proprietary software operating environments.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Considers practical applicability • Considers risk/vulnerability • Would be able to isolate cyber security requirements for control systems vs. other systems. • Definitely the way utilities see things. • Would allow for sane application of controls to equipment (not more inane requirements for mal-ware on a network switch!) • Would eliminate the need for TFE's • *Protection based on actual risks* • Yes, requirements MUST take into account the system they are being required on. • Focuses on specific types of software •	• Introduces (necessary?) complexity • May require updates as "proprietary" become general purpose • Definition of proprietary somewhat problematic • I think this will be confusing and complex for the drafting team to figure out. • I feel these two categories are too vague to separate. For instance, many devices run on some type of Linux distro without the end users knowledge. • Ultimately, we must work toward improving the overall security of all applications, whether they are general purpose or custom built • Future changes to environments may require entities to significantly change their security. • May introduce blind spots to security holes. • May trigger equipment changes to avoid implementing requirements (while this may be seen as "gaming", if it does not decrease or possibly improves the security posture, what is wrong with it?) • "General purpose" and "Proprietary" are problematic terms to define. • These apply mainly to technical controls, and I'm not sure there would be any difference in applicability for many of the controls. • *Possibly more complex* • Requires enumeration of these OS'es in the standard • Not clear why this is needed

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	4	**3**	**6**	**1**

Avg. =2.8

D. Consider a process for allowing entities to apply compensating security controls on the basis of a risk management program and approval process.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Practical and flexible • Details are important • More Flexibility for entities. • We have tried "reasonable business judgment" and TFEs because we acknowledge the need to apply appropriate controls on the basis of risk and the limitation of the SDT to draft perfect controls. In other words, we have to have something, and I don't think TFEs are it. • *Allows security risks to be managed differently* • If scope = all systems, this is essential. Meets the NIST framework, which is something we've been ordered to incorporate • Helps apply reasonability	• Subject to "gaming" • Difficult to monitor and enforce compliance • Has been tried before with adverse public perception • Not sufficiently specific. • Will result in some of the same problems we have today concerning leaving the interpretation up to the individual company. • At face value, this appears difficult to audit consistently. • The age old problem of who can ultimately provide approval. • Sounds suspiciously like TFE's, to me…and I'd rather get rid of them… • Who approves? • Risk management is hard or impossible to assess. • *More complex* • *Approval, by whom?* • A non-bright line, but I think it's necessary. • Danger that 'approval processes could turn into TFE on steroids nightmare.

			• Not sure industry would want to share the required sensitive details with an approving entity • Who would be the approver and what criteria would they use to say what is acceptable • Approval by whom?	
Acceptability Ranking Scale	***4** = acceptable**,** I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	2	**2**	**8**	**0**

Avg. =2.5

OTHER SCOPE AND APPLICABILITY PROPOSALS *(list below)*

SDT Member Comments

- We should refer to requirements (as opposed to controls).
- If I did not answer these questions right (the way you want this to go) will I still be allowed on the straw man team?
- We need to lay out security/reliability goals for each of the environments and then draft requirements/controls that meet those goals. For example, we need to have in mind what level of security needs to be in place at a high impact substation and what needs to be in place at a low impact substation. We need to lay out the nine possibilities (Gen/Trans/Control Center and an L/M/H of each) and determine what we are shooting for in each. Only then, with these agreed upon goals in mind, can we split off into different teams looking at different areas of controls. The old "Begin with the end in mind" thing.

Other Approaches-

Thomas M. Overman, Boeing

The grid will be either integrated or stove-piped. Subjecting Generation, Transmission & Distribution to separate requirements will limit the desired integration of the Smart Grid.

Consider another approach:

- Safety of life (protection of line crews, public{primarily from hydro ops}, mechanics, operators, etc)
- System stability (national, regional, local)
- Equipment protection (Major affecting national capabilities (large generating plant and equipment, NW-SW Intertie, 4C sub, etc), medium affecting regional or large municipal supplies, local affecting city/county)
- Business operations (IT, metering, etc)

Appendix # 7
SECURITY CONTROLS SUB-TEAM MEMBER PREFERENCE FORM
JANUARY 20, 2010

SDT Member Preferences: Rob Antonishen (RA), Jeri Domingo Brewer (JDB)Jim Brenton (JB), Jackie Collett(JC), Jay Cribb (JCr), Joe Doetzl (JD), Sharon Edwards (SE), Jeff Hoffman(JH)
Jerry Freese (JF) Phil Huff(PH) Doug Johnson (DJ) Rich Kinas(RK), David Revill(DR), Kevin Sherlin (KS) Jon Stanford (JS),Keith Stouffer(KSt)) John Varnell (JV) Bill Winters(BW)

Sub-Team	Preference Order #1 through #6	Control Families
A. Security Governance and Assessments Jon Stanford, Rich Kinas, Jerry Freese, *Dave Norton & John LIm*	**JS (1) RK(1) KSt(1) JF(1) PH(1) JDB(2) JH(2)**SE(3)JB(4)JC KS(4)(5) DR (5) JCr(5)RA(5) JV(5)BW(5) DJ(6)	Security Governance *(CIP 003- R1, R2, R3)* Security Assessments *(CIP 005, R4, CIP 007 R 8*
B. Personnel and Physical Security Doug Johnson, Rob Antonishen, Kevin Sherlin	**DR (1) DJ(1)RA(1) KS(1) JF(2)** JS(3) JH(3)JDB(4)JB(5)SE(5) JC (6) JCr(6)JV(6)RK (6)KSt(6) PH(6) BW(6)	Personnel and Training *(CIP 004 R 1, R2, R3)*, (4) Physical Security *(CIP 006 R1-R6)*
C. Operations Security Jay Cribb, Jim Brenton, John Varnell, Jackie Collett	**JC (1) JCr(1) JV(1) JB(1), JDB(1) JH(1) BW(1)KS(2)RK(2)KSt(2)SE(2)RA(2)** DR(3)PH(3)DJ(3)JF(4) JS(5)	Communication Protection *(CIP 005 R1, R3)*, Systems Management *(CIP 007 R2, R3, R4, R6)*
D. Recovery and Response Scott Rosenberger Jeri Brewer, , Joe Doetzl	**JS(2)** JC (3) BW(3) JDB(3)JCr(4) JV(4) DJ(5) KS(5)RK(5)KSt(5)PH(5)JH(5)DR (6) JB(6) JF(6)SE(6)RA(6)	Incident Response (*CIP 008 R1 R2)*, (7) Recovery Plans *(CIP 009, R1-R5)*
E. Access Control and Auditing Sharon Edwards, Phil Huff, Jeff Hoffman	**SE(1)JC (2) JB(2) DJ(2) JCr (2) PH(2) JV(2)**RK(3)DR (4) RA(4) JS(4)KSt(4)JF(5) KS(6) JDB(6)JH 6) BW(4)	Access Control, (*CIP 003, R5, CIP 005 R2, CIP-007 R5, CIP 004 R4* Audit and Accountability *CIP 005 R5, CIP 007 R9)*
F. Change Management, System Lifecycle and Information Management Dave Revill, Keith Stouffer, Bill Winters	**DR (2) BW(2)** KSt(3)JF(3) JB(3)JCr(3)JV(3) KS(3)RA(3)JC(4) DJ (4) RK(4)SE(4)PH(4)JDB(5)JS(6)JH (4)	Configuration Management and System Lifecycle *(CIP 003, R6, CIP 007 R1, R7)* (11) Information Management *(CIP 005 R4, CIP 007 R8)*

Appendix #8 Security Controls Strawman Document

SECURITY CONTROL DRAFTING PRINCIPLES

GUIDANCE IN DRAFTING SECURITY CONTROLS TO ENSURE A CONSISTENT OUTCOME AMONG SUB-TEAMS

Drafting Principles

16. **Applicability [NERC Rules of Procedure[6]] –** 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. Such functional classes include: reliability coordinators, balancing authorities, transmission operators, transmission owners, generator operators, generator owners, interchange authorities, transmission service providers, market operators, planning authorities, transmission planners, resource planners, load-serving entities, purchasing-selling entities, and distribution providers. Each reliability standard shall also identify the geographic applicability of the standard, such as the entire North American bulk power system, an interconnection, or within a regional entity area. A standard may also identify any limitations on the applicability of the standard based on electric facility characteristics.
17. **Reliability Objective [NERC Rules of Procedure] –** 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. The following general objectives for the bulk power system provide a foundation for determining the specific objective(s) of each reliability standard:
    a. **Security** – Bulk power systems shall be protected from malicious physical or cyber attacks.
18. **Performance Requirement or Outcome [NERC Rules of Procedure]** – 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. Each requirement is not a "lowest common denominator" compromise, but instead achieves an objective that is the best approach for bulk power system reliability, taking account of the costs and benefits of implementing the proposal
19. **Measurability [NERC Rules of Procedure] –** 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. Each performance requirement shall have one or more associated measures used to objectively evaluate compliance with the requirement. If performance can be practically measured quantitatively, metrics shall be provided to determine satisfactory performance.
20. **Technical Basis in Engineering and Operations [NERC Rules of Procedure] –** Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.
21. **Completeness [NERC Rules of Procedure] –** Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.
22. **Consequences for Non-Compliance[NERC Rules of Procedure] –** 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.
23. **Clear Language [NERC Rules of Procedure] –** 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.

[6] *Rules of Procedure of the NERC*, June, 16th, 2009, pp. 6, 7

24. **Practicality [NERC Rules of Procedure] –** Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
25. **Consistent Terminology [NERC Rules of Procedure] –** 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.
26. **Reduce Risk** [**3.5 acceptability among survey respondents**] **–** Security controls reduce risk appropriately for applicable BES impact categories
27. **Change Documentation** [**3.3 acceptability among survey respondents**] – 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
    c. Major formatting changes
28. **Reduce Administrative Overhead** [**Suggested principle**] **–** Administrative documentation kept to the minimum that is necessary to verify acceptable risk
29. **Priority [Suggested Principle] –** Implementation and compliance with the Standards are prioritized according to BES risk. The industry should focus on mitigating the greatest risk (i.e. not spend the majority of our resources on the low-impact Cyber Systems).
30. **Minimize TFEs** [**Suggested principle**] **–** Security controls should minimize the need for TFEs

Security Control Groups

Control groups are split initially by the CIP Standards, and additional control groups (8-13) are pulled out to prevent cross-Standard references. Each control group has the relevant CIP and 800-53 families mapped. This approach should reflect the team's consensus to:

> *"Begin with the current CIP-003 to 009 requirements review and document the applicable Order 706 directives and review any new ways to combine and select those NIST SP 800-53 controls that should be used in a new CIP set of controls."*

ID	Control Group	NERC Standard	NIST 800-53 Family
1	Security Governance	CIP-003 – R1, R2, R3;	Planning, Risk Assessment, Program Management
2	Personnel and Training	CIP-004 – R1, R2, R3	Awareness and Training, Personnel Security
3	Communication Protection	CIP-005 R1, R3	System and Communication Protection
4	Physical Security	CIP-006 R1 through R6	Physical and Environmental Protection
5	Systems Management	CIP-007 R2, R3, R4, R6	System and Information Integrity
6	Incident Response	CIP-008 R1 & R2	Incident Response
7	Recovery Plans	CIP-009 R1 through R5	Contingency Planning
8	Access Control (Technical)	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4	Access Control, Identification and Authentication
9	Audit and Accountability	CIP-005 R5, CIP-007 R9	Audit and Accountability
10	Configuration Management and System Lifecycle	CIP-003 R6; CIP-007 R1, R7	Configuration Management, Maintenance, Media Protection, System and Services Acquisition
11	Information Management	CIP-003 R4	Access Control, Media Protection
12	Security Assessments	CIP-005 R4, CIP-007 R8	Security Assessment and Authorization

Drafting Sub-Teams
Additional members may be necessary for teams that have a large number of requirements or FERC directives allocated.

Team	Control Families
Security Governance	(1) Security Governance
Personnel and Physical Security	(2) Personnel and Training, (4) Physical Security
Operations Security	(3) Communication Protection, (5) Systems Management
Recovery and Response	(6) Incident Response, (7) Recovery Plans , (12) Security Assessments
Access Control and Auditing	(8) Access Control, (9) Audit and Accountability
Change Management, System Lifecycle and Information Management	(10) Configuration Management and System Lifecycle, (11) Information Management

Team Assignments

Each team shall assemble the following documentation as part of their drafting assignments. The additional documentation should assist in (1) maintaining consistency across the teams and (2) presenting the purpose and background of the security controls to the industry.

Each team should begin by determining the security controls within their assigned control families necessary to mitigate risk to the BES. Begin by taking the set of applicable Requirements from version 3 CIP Cyber Security Standards and reconcile with applicable NIST 800-53 security controls. Then incorporate additional sources where applicable to mitigate unacceptable risk to the BES functions.

The initial work product should be a set of security controls with applicability to high, medium and low impact Cyber Systems and how specific FERC directives have been addressed (as indicated in Appendix A: FERC Directives from Order 706).

Additionally, for each security control[7]:

7. **Statement of Risk –** State how the security control reduces risk appropriate to the impact categorization [**Drafting principle 11**]
8. **Measures –** State how an objective third party with knowledge or expertise in security can measure the control [**Drafting principle 4**]
9. **Change Documentation –** State the rationale for making changes from previous versions [**Drafting principle 12**]
10. Denote the applicability to (1) Generation Subsystems, (2) Transmission Subsystems, and (3) Control Centers. Provide clarifications or enhancements where necessary to meet the security control objective in that environment [**3.2 acceptability among survey respondents**].
11. Denote the priority for the security control relative to the risk it mitigates (i.e. P1, P2, P3, None). [**SP800-53 introduced this in version 3, and it could help in developing VRFs and implementation plans**]
12. *Team needs to discuss the following scoping exercise to determine how to accomplish these goals of applying appropriate security controls:*
    a. Denote applicability for differing vulnerability and threat profiles. Write controls based on risk profile (as well as impact categorization) [**2.9 acceptability among survey respondents**].
    b. Denote applicability for general purpose vs. proprietary operating systems [**2.8 acceptability among survey respondents**].

Security Controls for Impact Categories

This section provides guidance in the types of controls applicable to High, Medium and Low impact categories. The basic premise is that the cost to implement security controls should reflect the reduction of risk to the BES commensurate with the impact category. The industry as a whole should first focus on mitigating the greatest amount of risk.

Cost to Implement and Maintain / Risk Reduction (Benefit)	Significant	Moderate	Minimal
Signficant	Hi/Med	All	All
Moderate	Hi	Hi/Med	All
Minimal	N/A	Hi	Hi/Med

Figure 1: Applicability to Impact Categories based on Cost vs. Risk Reduction

CIP Security Profiles (Examples For Discussion Only)

Transmission Subsystems (aka substations. Environment = remote, unmanned locations)

[7] This section calls for specific documentation of only a few *Drafting Principles.* Other *Drafting Principles* provide evaluation criteria for security controls.

- **Low** *Primary Concern:* Attackers using it as a launching point to higher impact assets.
  - Controlled access to upstream networks
  - All passwords must be changed from manufacturer defaults on all devices that support a password.
  - No physical security requirements
- **Medium**
  - Same as low for subs??
- **High** *Primary Concern:* The substation is itself a target or a launching point.
  - Physical access control and logging.
  - Electronic access control and logging for all remote access. Strong authentication for remote access.
  - Little to no systems management in substation environment since it consists mostly of dedicated devices (IEDs). Make it mostly about strong access control both electronically and physically with notifications of unauthorized access.

Generation Subsystems (aka plants. Environment = Campus with widely distributed cyber components)

- **Low** *Primary Concern:* Upstream attacks
  - Controlled access to upstream networks (limit use as a launching point for attacks)
  - All passwords must be changed from manufacturer defaults on all devices that support a password.
- **Medium** *Primary Concern:* Attackers gaining control of multiple units within the plant.
  - Good segmentation with access control between individual generating units or groups of smaller units
- **High** *Primary Concern:* Attackers gaining control of multiple units within the plant or across several plants.
  - Strong, highly controlled segmentation between individual generating units.
  - Strong authentication required for all remote electronic access
  - Good systems management, change mgt, vulnerability mgt on control system servers, HMIs.

Control Centers (Environment = centralized data centers)

- **Low** *Primary Concern:* Attacks over their connectivity to higher impact control centers
  - Controlled access to other control networks.
  - Controlled physical access.
  - Vulnerability management on all systems that communicate outside ESP
- **Medium** *Primary Concern*: Same as low (only < 2000 MW centers)
  -
- **High** *Primary Concern:* The ultimate target – gaining control of numerous assets.
  - All the current requirements plus Order 706 changes plus what makes sense out of 800-53.
  - The strongest perimeters (physical and electronic)
  - Stringent systems management, change mgt, vulnerability mgt.
  - Strong personnel controls.

Sources

In order to develop a complete set of controls, all of the aforementioned Standards should be considered with the caveat that NERC CIP/NIST 800-53 serve as the baseline and SANS, ISO, DHS, and ISA-99 provide supplemental or amplifying guidance.

- DHS of Control Systems Security Recommendations for Standards Developers[8]
- Federal Information System Controls Audit Manual (FISCAM) Mapping to CIP Requirements[9]
- ISA 99[10]
- ISO/IEC 27001 & 27002[11]
- SANS 20 Critical Security Controls[12]

Appendix A: FERC Directives from Order 706

Paragraph	Text	Phase[13]	Team
25	we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	Version 4	ALL
253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance … leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	Guideline / Version 4	CIP-002
254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary]when developing the guidance.	Guideline / Version 4	CIP-002
257	we direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Guideline / Version 4	CIP-002
272	the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Guideline / Version 4	CIP-002
272	The Commission directs the ERO to develop guidance on the steps that	Guideline /	CIP-002

[8] http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf
[9] http://www.gao.gov/new.items/d09232g.pdf (FISCAM document only. CIP mapping available from NERC staff)
[10] http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821 (for purchase)
[11] http://www.27000.org (for purchase)
[12] http://www.sans.org/critical-security-controls/cag.pdf
[13] Schedule phases in this column mean one or more of the following:

- "Version 2" – complete in filed version 2
- "Version 4" – planned for next major version (12-18 months plus)
- "Guideline" – stand alone guidance started after corresponding requirement is determined
- "TFE Filing" – 2009 filing on TFE proposal and Appendix 4D to RoP
- "not scheduled" – beyond Version 4
- "CMEP" – part of an existing or ongoing compliance audit, self-report or other process
- "VRF Filing(s)" – one of several already-filed (or very soon to be filed in the case of Version 2) VRF and/or VSL filings

Phase may also be self-explanatory if not one of these entries

Paragraph	Text	Phase[13]	Team
	would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Version 4	
282	the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	Guideline / Version 4	CIP-002
285	we direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable – by testing and experience].	Version 4	ALL
322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0	CIP-002
329	the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0	CIP-002
376	the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 4	CIP-002
386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 4	Access Control and Auditing
397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 4 / Guideline	Change Management, System Lifecycle and Information Management
433	we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 4	Personnel and Physical Security
434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.	Version 4	Personnel and Physical Security
435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to	Version 4	Personnel and Physical

Paragraph	Text	Phase[13]	Team
	assure that security trainers are adequately trained themselves.		Security
443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 4	Security Governance
460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 4	Personnel and Physical Security
464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 4	Personnel and Physical Security
473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	Version 4	Security Governance
476	we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent	Version 4	Security Governance
511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 4	Operations Security
525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days	Version 4	Access Control and Auditing
526	the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 4	Access Control and Auditing
526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 4	Access Control and Auditing
528	the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 4	Access Control and Auditing
541	we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 4	Recovery and Response
542	the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 4	Recovery and Response
544	the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant	Version 4	Recovery and Response

Paragraph	Text	Phase[13]	Team
	change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.		
544	we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment	Version 4	Recovery and Response
547	we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	Version 4	Recovery and Response
581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 4	Recovery and Response
609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	Version 4 / Guideline	Change Management, System Lifecycle and Information Management
610	we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 4	Change Management, System Lifecycle and Information Management
611	the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 4	Change Management, System Lifecycle and Information Management
619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	Version 4 / not scheduled	Operations Security
622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	Version 4 / not scheduled	Operations Security
628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed	Version 4	Access Control and Auditing

Paragraph	Text	Phase[13]	Team
	more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1		
629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 4 / guideline	Access Control and Auditing
633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.	Version 4	Change Management, System Lifecycle and Information Management
635	the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4	Change Management, System Lifecycle and Information Management
661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced	Version 4 / Guideline	Recovery and Response
673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 / Guideline	Recovery and Response
676	the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 /. Guideline	Recovery and Response
686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.	Version 4	Recovery and Response
686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 4	Recovery and Response
694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 4	Recovery and Response
694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in	Version 4	Recovery and Response

Paragraph	Text	Phase[13]	Team
	compliance with this Reliability Standard.		
739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 4	Recovery and Response
748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use.	Version 4	Recovery and Response

Appendix #9 Communication Plan

Communications Plan for Cyber Security Order 706 Project – Version 4

Background

On January 18, 2008, the Federal Energy Regulatory Commission (FERC) issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection standards (CIP-002-1 through CIP-009-2). In the Order, FERC also directed numerous modifications to the standards. NERC initiated Project 2008-06 – Cyber Security Order 706, whose scope includes addressing the FERC directives in Order No. 706. The drafting team assembled for this project segmented the scope of work into multiple phases: Versions 2 and 3 of the CIP standards addressed timely FERC directives regarding reasonable business judgment and other non-controversial issues. The bulk of the Order No, 706 directives are to be addressed in Version 4 of the standards. NERC's objective is to produce an approved revision to CIP-002 by June, 2010 and revisions to CIP-003 through CIP-009 by the end of 2010.

NERC and especially the drafting team recognizes that effective communications regarding the ongoing work of the team is crucial to the success of the project and is vital to achieving the consensus necessary for passage in the balloting process.

Mission

Inform and educate reliability stakeholders about Version 4 of the Project 2008-06 — Cyber Security Order 706 standards project, and promote input and participation from stakeholders and regulators.

Scope/Objectives

1. Obtain stakeholder (industry and government) buy-in by communicating importance of Version 4 of the CIP-002 through CIP-009 reliability standards:
    a. communicate paradigm shift in approach to Version 4 relative to prior versions
    b. communicate benefits to reliability
    c. justify commitment of resources
    d. justify aggressive schedule for completion in 2010
2. Ensure key audiences (FERC, trade groups, NERC committees) are kept abreast of the drafting team's plans, successes, and challenges
3. Prepare industry stakeholders, in particular the Registered Ballot Body, to respond promptly and fully to requests for comment and ballots by providing adequate information about drafting team discussions and decisions as they occur
4. Create a feedback clearinghouse to determine information gaps and develop FAQ, where necessary

Audience

- All NERC registered entities held to compliance with NERC CIP-002 through CIP-009 reliability standards
- NERC standards, compliance, and other relevant staff (ex. Standard Coordinators, Compliance Registry, Enforcement, etc)
- NERC Member Representatives Committee
- NERC Standing Committees and relevant taskforces, ad hoc groups, subcommittees, and contractors (ex. Operating Committee, Planning Committee, Critical Infrastructure Protection Committee)
- Regional Entity staff and committees (ex. equivalent of NERC Standards Committee)
- Regional Entity management group
- FERC Commissioners, Office of Electric Reliability staff, and Office of Enforcement staff

- Industry executives (senior managers and CEOs)
- Line employees, subject matter experts, and members of standard drafting teams
- Trade associations (EEI, APPA, NRECA, EPSA, ELCON, NARUC)
- Public Utility Commissions

Topics

Concepts	• Core aspects of CIP-002-4: categorizing cyber systems based on BES reliability functions; • Core aspects of CIP security controls (requirements) based on cyber system categorization (CIP-003-4 through CIP-009-4)
Benefits and importance	• demonstrate the criticality of project success in 2010 to NERC's overall success • improve the overall quality and robustness of the NERC critical infrastructure protection standards • more objective determination (bright line thresholds) of asset categorization for applying security controls • positive impact on overall reliability of the grid • benefits to stakeholders by demonstrating ability to produce good standards timely • obtain CEO-level support for project that is communicated throughout organizations
Resources	• what resources are needed to support the drafting team in producing Version 4 technically and administratively • when and for how long
Timeline	• CIP-002-4 ballot completed by end of May, 2010 • CIP-003-4 through CIP-009-4 ballot completed by end of 2010
Impact on process	• what will be different in the drafting, reviewing, and balloting process for these Version 4 CIP standards as opposed to other typical standards projects • import of external support to facilitate drafting team efficiency, e.g. facilitation, technical writing, etc. • impact of resource commitment to Project 2008-06 may impact support for other active projects
Information sources	• where stakeholders can get further information as project proceeds in 2010 • provide access to message packages as they are available (especially for trade groups)

Delivery Methods

e-mail	• use distribution lists to ensure full coverage (NERC, Regional Entities, etc.) • use Regional Entity distribution lists to reach targeted personnel
Webinars	• associated with each posting of the standards for comment; o conduct for each significant proposal/modification for which comment is requested • record and "distribute/make available" for those who cannot attend

	• include feedback option (on demand after structured presentation/Webinar)
Committee meetings (NERC, Regional)	• attend meetings and communicate message • request special call if necessary for briefing
NERC Web site	• centralized place; linked from Regional Entity sites • headline news, big button on home page (similar to "Renewables"), pop-up page, project page, standards under development, and other frequently hit pages
Structured conference call and/or meeting	for standards drafting team representatives and NERC coordinators, including contractors;
Face-to-face outreach	• e.g. trade groups, FERC commissioners and staff, Regional Entities, committees • high-level involvement from NERC • goal: discuss Version 4 standards project with each trade organization, and at each Regional Entity general meeting at least once in spring and once in Fall, 2010.
"Canned message"	• slides and presentations (project information – overview, etc.) • files accessible via Web site and possible in-person delivery of recorded message
Press releases	As significant milestones are achieved – e.g. ballot approval, NERC Board approval, regulatory approval.
Newsletters	Monthly NERC News updates; Regional Entity newsletters
Workshops	• Include as agenda item on regional workshops • Special Cyber Workshop (?) • NERC Standards workshop (Fall 2010)
Regional Entity management group meetings/calls	Group holds weekly (Friday) conference calls and meets face-to-face prior to certain high-level meetings – standing committees, BOT Ask Regional Entity Mangers to discuss the initiative at various conferences they attend to relay the message and gain additional support from stakeholders

Delivery Plan/Timeline

Planned Tactics:

Date	Tactic	Audience	Content Developer(s)	Presenter/Delivery
January 22, 2010	Announce NERC-sponsored Webinar	Industry	Carl Dombek, Gerry Adamski	Carl Dombek, Gerry Adamski
January 25, 2010	Submit communications plan to drafting team for endorsement	Drafting team	Gerry Adamski	Gerry Adamski
End of January 2010	Review and revise web page for high-level updates (with links from home page and standards pages)	Industry/FERC	Gerry Adamski, Carl Dombek,	Gerry Adamski
Periodically	Provide custom NERC cyber newsletter on development efforts	Industry	Joe Bucciero	Joe Bucciero
February 2010	Develop a frequently asked questions document for Web page	All	Drafting team	Drafting team
February 3, 2010, 1 PM EST	Conduct industry webinar to discuss CIP-002-4 draft	Industry	Standard Drafting Team	Philip Huff, et al.
February 15, 2010	Provide status update	MRC and NERC Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
February 19 2010	Develop talking points and core messages that would be used in various levels of detail for all communications for CIP-002-4 posting and for CIP-003-4 through CIP-009-4 development.	All	Standard Drafting Team members TBD, NERC staff (Carl Dombek), NERC regional communications group	TBD
February - December 2010	Provide individual briefings on anticipated process and schedule	Electric trade associations, regional entity member meetings, FERC Reliability	Gerry Adamski, Mike Assante, Drafting Team leaders	Gerry Adamski, Mike Assante, Drafting Team leaders

Date	Tactic	Audience	Content Developer(s)	Presenter/Delivery
	Obtain feedback	Office		
March 16-18, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
Early April 2010	Conduct (and record) Webinar held on CIP-003-4 through CIP-009-4. Solicit feedback during Webinar	Industry	Drafting team, NERC staff	Drafting team members TBD
April, 2010	Issue Cauley letter to executive leadership of organizations sponsoring drafting team members expressing appreciation for commitment	Drafting team executive organizational leadership	Carl Dombek, Gerry Adamski	Gerry Cauley
April 2010	Announce NERC-sponsored CIP-003-4 through CIP-009-4 in-person technical conference	Industry	Carl Dombek, Gerry Adamski	Carl Dombek, Gerry Adamski
May 11, 2010	Provide drafting team status report to NERC MRC at May meeting (include assessment of ability to meet targets)	NERC MRC and Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
May. 2010	Issue news release on positive ballot results for CIP-002-4	All	Gerry Adamski, Carl Dombek	Carl Dombek
May 2010	Issue Cauley letter to stakeholders expressing appreciation for support	Stakeholders	Gerry Adamski; Carl Dombek	Gerry Cauley
June/July 2010	Conduct NERC-sponsored CIP-003-4 through CIP-009-4 in-person technical conference Solicit feedback during Webinar	Industry	Drafting team	Drafting team
June/July 2010	Review efforts conducted through June and draft plan for remainder of year	Communications team	Carl Dombek, Gerry Adamski, Drafting Team leadership	Carl Dombek

Date	Tactic	Audience	Content Developer(s)	Presenter/Delivery
June 15-17, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
August 4, 2010	Provide status update	MRC and NERC Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
August, 2010	Announce webinar in support of CIP-003-4 through CIP-009-4	Industry	Carl Dombek, Gerry Adamski	Carl Dombek, Gerry Adamski
August 2010	Conduct webinar in support of CIP-003-4 through CIP-009-4	Industry	Standard Drafting Team	Philip Huff, et al.
September 14-17, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
November 3, 2010	Provide status update	MRC and NERC Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
December 7-9, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
December. 2010	Issue news release on positive ballot results for CIP-003-4 through CIP-009-4	All	Gerry Adamski, Carl Dombek	Carl Dombek
December 2010	Issue Cauley letter to stakeholders expressing appreciation for support	Stakeholders	Gerry Adamski; Carl Dombek	Gerry Cauley